kaspersky

# Kaspersky Security Center 17 Linux

© 2026 AO Kaspersky Lab

# Contents


Kaspersky Security Center Linux Help

What's new

Fixed issues

About Kaspersky Security Center Linux

- Distribution kit
- Hardware and software requirements
  - Administration Server requirements
  - Web Console requirements
  - Network Agent requirements
- Compatible Kaspersky applications and solutions
- About compatibility of Kaspersky Security Center Linux components
- Comparison of Kaspersky Security Center: Windows-based vs. Linux-based
- About Kaspersky Next Expert View

Architecture and basic concepts

- Architecture
- Deployment diagram of Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console
- Ports used by Kaspersky Security Center Linux
- Ports used by Kaspersky Security Center Web Console
- Basic concepts
  - Administration Server
  - Hierarchy of Administration Servers
  - Virtual Administration Server
  - Web Server
  - Kaspersky Security Center Linux Web Server
  - Network Agent
  - Administration groups
  - Managed device
  - Unassigned device
  - Administrator's workstation
  - Management web plug-in
  - Policies
  - Policy profiles
  - Tasks
  - Task scope
  - How local application settings relate to policies
  - Distribution point
  - Connection gateway
  - Virtual Administration Servers

Schemas for data traffic and port usage

- Administration Server and managed devices on a local area network (LAN)
- Primary Administration Server on LAN and two secondary Administration Servers
- Administration Server on LAN, managed devices on internet, reverse proxy in use
- Administration Server on LAN, managed devices on internet, connection gateway in use

- Administration Server in DMZ, managed devices on internet
- Interaction of Kaspersky Security Center Linux components and security applications: more information
  - Conventions used in interaction schemas
  - Administration Server and DBMS
  - Administration Server and client device: Managing the security application
  - Upgrading software on a client device through a distribution point
  - Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server
  - Hierarchy of Administration Servers with a secondary Administration Server in DMZ
  - Administration Server, a connection gateway in a network segment, and a client device
  - Administration Server and two devices in DMZ: a connection gateway and a client device
  - Administration Server and Kaspersky Security Center Web Console
- Getting started
  - Hardening Guide
    - Hardening checklist
    - Administration Server deployment
    - Connection safety
    - Accounts and authentication
    - Managing protection of Administration Server
    - Managing protection of Network Agent
    - Managing protection of client devices
    - Configuring protection for managed applications
    - Administration Server maintenance
    - Event transfer to third-party systems
    - Security recommendations for third-party information systems
    - Recommendations for using Kaspersky security applications
    - Scenario: Authenticating MySQL Server
    - Scenario: two-way TLS authentication of PostgreSQL for the Administration Server database and the IAM database
  - Preparation for deployment
    - Selecting the configuration of Kaspersky Security Center Linux
      - Standard configuration: Single office
      - Standard configuration: A few large-scale offices run by their own administrators
      - Standard configuration: Multiple small remote offices
    - Selecting a structure for protection of an enterprise
    - Typical schemes of protection system deployment
    - Selecting a DBMS
    - Providing internet access to Administration Server
      - Internet access: Administration Server on a local network
      - Internet access: Administration Server in DMZ
  - Installation
    - Configuring the MariaDB x64 server for working with Kaspersky Security Center Linux
    - Configuring a PostgreSQL-based DBMS server to work with Kaspersky Security Center Linux
    - Configuring the MySQL x64 server for working with Kaspersky Security Center Linux
    - Preparing a high availability DBMS cluster for working with Kaspersky Security Center Linux
    - Installing Kaspersky Security Center Linux
      - Installing Kaspersky Security Center Linux in silent mode
      - Installing Kaspersky Security Center Linux on Astra Linux in the closed software environment mode

Installing Kaspersky Security Center Web Console
Kaspersky Security Center Web Console installation parameters
Installing Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode
Installing Kaspersky Security Center Linux with a script
Deployment of the Kaspersky Security Center Linux failover cluster
Kaspersky Security Center Linux failover cluster. Deployment schemes
Kaspersky Security Center Linux failover cluster
Scenario: Deployment of Kaspersky Security Center Linux failover cluster
Kaspersky Security Center Linux failover cluster. Hardware and software requirements
Preparing a file server for a Kaspersky Security Center Linux failover cluster
Preparing nodes for a Kaspersky Security Center Linux failover cluster
Installing Kaspersky Security Center Linux on the Kaspersky Security Center Linux failover cluster nodes
Starting and stopping cluster nodes manually
Reinstalling a failover cluster node
Installing Kaspersky Security Center Web Console connected to Administration Server installed on Kaspersky Security Center Linux failover cluster nodes
Geo-distributed Kaspersky Security Center Linux failover cluster
Geo-distributed cluster running Ubuntu with PostgreSQL DBMS
Preparing a file system of cluster nodes
Configuring a replicated cluster file system
Installing and configuring Corosync and Pacemaker on the cluster nodes
Installing and configuring the PostgreSQL DBMS
Installing Kaspersky Security Center Linux on the geo-distributed failover cluster nodes
Geo-distributed cluster running SberLinux with Platform V Pangolin DBMS
Preparing a file system of cluster nodes
Configuring a replicated cluster file system
Installing and configuring Corosync and Pacemaker on the cluster nodes
Installing and configuring the Platform V Pangolin DBMS
Installing Kaspersky Security Center Linux on the geo-distributed failover cluster nodes
Installing Kaspersky Security Center Web Console on geo-distributed failover cluster nodes
Accounts for working with the DBMS
Creating MySQL and MariaDB databases and user accounts
Creating PostgreSQL-based databases and user accounts
Moving data from a shared tablespace to a file-per-table tablespace in a MySQL or MariaDB DBMS
Certificates for work with Kaspersky Security Center Linux
About Kaspersky Security Center certificates
Requirements for custom certificates used in Kaspersky Security Center Linux
Reissuing the internal certificates for Kaspersky Security Center Web Console
Replacing certificate for Kaspersky Security Center Web Console
Converting a PFX certificate to the PEM format
Scenario: Specifying the custom Administration Server certificate
Replacing the Administration Server certificate by using the klsetsrvcert utility
Connecting Network Agents to Administration Server by using the klmover utility
Reissuing the Web Server certificate
Changing the default IAM certificate to a custom one
Adding the Administration Server address to the IAM Server configuration
Defining a shared folder

Signing in to Kaspersky Security Center Web Console and signing out
Kaspersky Security Center Web Console interface
Changing the language of the Kaspersky Security Center Web Console interface
Changing the Kaspersky Security Center Web Console home page
Adding and removing bookmarks
Removing Kaspersky Security Center Web Console
Quick start wizard
Step 1. Specifying the internet connection settings
Step 2. Downloading required updates
Step 3. Selecting the assets to secure
Step 4. Selecting encryption in solutions
Step 5. Configuring installation of plug-ins for managed applications
Step 6. Downloading distribution packages and creating installation packages
Step 7. Configuring Kaspersky Security Network
Step 8. Selecting the application activation method
Step 9. Specifying the third-party update management settings
Step 10. Creating a basic network protection configuration
Step 11. Configuring email notifications
Step 12. Closing the quick start wizard
Protection deployment wizard
Step 1. Starting Protection deployment wizard
Step 2. Selecting the installation package
Step 3. Selecting a method for distribution of key file or activation code
Step 4. Selecting Network Agent version
Step 5. Selecting devices
Step 6. Specifying the remote installation task settings
Step 7. Restart management
Step 8. Removing incompatible applications before installation
Step 9. Moving devices to Managed devices
Step 10. Selecting accounts to access devices
Step 11. Starting installation
Upgrading Kaspersky Security Center Linux
Upgrading Kaspersky Security Center Linux from version 16 or later
Upgrading Kaspersky Security Center Linux from version 16 or later by using the installation file
Upgrading Kaspersky Security Center Linux from version 16 or later through backup
Upgrading Kaspersky Security Center Linux from version 16 or later on the Kaspersky Security Center Linux failover cluster nodes
Upgrading Kaspersky Security Center Linux from version 15.4 or earlier
Upgrading Kaspersky Security Center Linux from version 15.4 or earlier by using the installation file
Upgrading Kaspersky Security Center Linux from version 15.4 or earlier through backup
Upgrading Kaspersky Security Center Linux from version 15.4 or earlier on the Kaspersky Security Center Linux failover cluster nodes
Upgrading Kaspersky Security Center Web Console
Upgrading Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode
Migration to Kaspersky Security Center Linux
General guide for migration to a new Kaspersky Security Center Linux server
Scenario for migration to Kaspersky Security Center Linux using the quick installation script.

Migration to Kaspersky Security Center by using the Migration wizard
Exporting group objects from Kaspersky Security Center Windows
Importing the export file to Kaspersky Security Center Linux
Switching managed devices to be under management of Kaspersky Security Center Linux
Configuring Administration Server
Configuring the Administration Server connection address
Configuring the connection of Kaspersky Security Center Web Console to Administration Server
Configuring an allowlist of IP addresses to connect to Kaspersky Security Center Linux
Configuring internet access settings for Administration Server
Hierarchy of Administration Servers
Creating a hierarchy of Administration Servers: adding a secondary Administration Server
Viewing the list of secondary Administration Servers
Managing virtual Administration Servers
Creating a virtual Administration Server
Enabling and disabling a virtual Administration Server
Assigning an administrator for a virtual Administration Server
Changing the Administration Server for client devices
Deleting a virtual Administration Server
Configuring Administration Server connection events logging
Setting the maximum number of events in the event repository
Moving Administration Server to another device
Changing the Administration Server name
Preserving connections by adding a new DNS record
Preserving connections by switching to IP address-based connectivity
Restoring interrupted connections after changing the server name
Changing DBMS credentials
Backup copying and restoration of the Administration Server data
Creating an Administration Server data backup task
Using the klbackup utility to back up and recover data
Using the klbackup utility to switch managed devices under management of another Administration Server
Backup and restoring Administration Server data when using MySQL or MariaDB
Administration Server maintenance
Deleting a hierarchy of Administration Servers
Access to public DNS servers
Configuring the interface
Encrypted connection to an Administration Server
Encrypt communication with TLS
Network settings for interaction with external services
Global list of subnets
Checking the integrity of modules by using the klscmodchk and integrity_checker utilities
Discovering networked devices
Scenario: Discovering networked devices
Windows network polling
IP range polling
Adding and modifying an IP range
Zeroconf polling
Domain controller polling

- Authentication and connection to a domain controller
- Configuring domain authentication for the Administration Server using flags
- Configuring a Samba domain controller
- Equipment inventory
  - Adding information about new devices
  - Configuring criteria used to define enterprise devices
- Using VDI dynamic mode on client devices
  - Enabling VDI dynamic mode in the properties of an installation package for Network Agent
  - Moving devices from VDI to an administration group

Managing client devices

- Settings of a managed device
- Manually checking the connection between a client device and the Administration Server. klnagchk utility
- Device moving rules
  - Creating device moving rules
  - Copying device moving rules
  - Conditions for a device moving rule
- Adding devices to an administration group manually
- Moving devices or clusters to an administration group manually
- About clusters and server arrays
- Properties of a cluster or server array
- Adjustment of distribution points and connection gateways
  - About distribution points
  - Standard configuration of distribution points: Single office
  - Standard configuration of distribution points: Multiple small remote offices
  - Calculating the number and configuration of distribution points
  - Assigning distribution points automatically
  - Assigning distribution points manually
  - Adding a connection gateway in the DMZ as a distribution point
  - Modifying the list of distribution points for an administration group
  - Enabling a push server
  - Increasing the limit of file descriptors for the klnagent service
- About device statuses
- Configuring the switching of device statuses
- Device selections
  - Viewing the device list from a device selection
  - Creating a device selection
  - Configuring a device selection
  - Exporting the device list from a device selection
  - Removing devices from administration groups in a selection
- Device tags
  - Creating a device tag
  - Renaming a device tag
  - Deleting a device tag
  - Viewing devices to which a tag is assigned
  - Viewing tags assigned to a device
  - Tagging a device manually
  - Removing an assigned tag from a device

Viewing rules for tagging devices automatically
Editing a rule for tagging devices automatically
Creating a rule for tagging devices automatically
Running rules for auto-tagging devices
Deleting a rule for tagging devices automatically
Managing device tags by using the klscflag utility
Data encryption and protection
Viewing the list of encrypted drives
Viewing the list of encryption events
Creating and viewing encryption reports
Granting access to an encrypted drive in offline mode
Transmitting encryption keys between Administration Servers
Changing the Administration Server for client devices
Avoiding conflicts between multiple Administration Servers
Moving devices connected to Administration Server through connection gateways to another Administration Server
Viewing and configuring the actions when devices show inactivity
Sending messages to device users
Turning on, turning off, and restarting client devices remotely
Remote access to managed devices
Remote access from a Linux-based device with Kaspersky Security Center Web Console to a Linux-based managed device
Remote access from a Linux-based device with Kaspersky Security Center Web Console to a Windows-based managed device
Remote access from a Windows-based device with Kaspersky Security Center Web Console to a Linux-based managed device
Remote access from a Windows-based device with Kaspersky Security Center Web Console to a Windows-based managed device
Mobile Device Management
Using Firebase Cloud Messaging
Integration with Public Key Infrastructure
Managing administration groups
Creating administration groups
Automatic installation of applications on devices in an administration group
Moving administration groups
Deleting administration groups
Deploying Kaspersky applications
Scenario: Kaspersky applications deployment
Adding management plug-ins for Kaspersky applications
Packages
Downloading and creating installation packages for Kaspersky applications
Creating installation packages from a file
Creating stand-alone installation packages
Network Agent installation package settings
Running stand-alone packages created by Kaspersky Security Center Linux
Installing applications by using stand-alone packages
Suitability of databases updating in an installation package of a security application
Changing the limit on the size of custom installation package data

Distributing installation packages to secondary Administration Servers
Viewing the list of stand-alone installation packages
Installing Network Agent for Linux
Preparing a Linux device for installation of Network Agent
Preparing a device running SUSE Linux Enterprise Server 15 for installation of Network Agent
Preparing a device running Astra Linux in the closed software environment mode for installation of Network Agent
Preparing to install Network Agent on a Linux operating system with glibc 2.5 (legacy OS)
Preparing to install Network Agent on a Linux operating system with OpenSSH version 6.4 (legacy OS)
Installing Network Agent on a Linux device remotely
Installing Network Agent for Linux in silent mode (with an answer file)
Installing Network Agent for Linux in interactive mode
Support of file system rollback for devices with Network Agent
Installing Network Agent for Windows
Installing Network Agent for Windows in interactive mode
Installing Network Agent for Windows in silent mode
Deployment by capturing and copying the image of a device
Network Agent disk cloning mode
Network Agent installation parameters
Installing applications using a remote installation task
About remote installation tasks in Kaspersky Security Center Linux
Installing an application remotely
Remote installing of applications on macOS devices
Installing applications on secondary Administration Servers
Remote installation of applications on devices with Network Agent installed
Managing device restarts in the remote installation task
Forced deployment through the remote installation task of Kaspersky Security Center Linux
Installing applications in silent mode
Preparing a macOS device for remote installation of Network Agent
Virtual infrastructure
Tips on reducing the load on virtual machines
Support of dynamic virtual machines
Support of virtual machines copying
Specifying settings for remote installation on Unix devices
Monitoring the deployment
Starting and stopping Kaspersky applications
Replacing third-party security applications
Removing applications or software updates remotely
Preparing a Windows device for remote installation
Creating Execute scripts remotely task
Creating an installation package based on a manifest file
Preparing an archive for Execute scripts remotely task
Remotely installing applications on devices using the Execute scripts remotely task
Configuring notifications and monitoring for the Execute scripts remotely task
Licensing
Licensing of Kaspersky Security Center Linux
About the End User License Agreement
About the license

- About the License Certificate
- About the license key
- Viewing the Privacy Policy
- Kaspersky Security Center licensing options
- About the key file
- About data provision
- About the subscription
- Activating Kaspersky Security Center Linux
- Licensing of managed Kaspersky applications
- Licensing of managed applications
- Adding a license key to the Administration Server repository
- Deploying a license key to client devices
- Automatic distribution of a license key
- Viewing information about license keys in use
- Events of the license limit exceeded
- Deleting a license key from the repository
- Revoking consent with an End User License Agreement
- Renewing licenses for Kaspersky applications
- Using Kaspersky Marketplace to choose Kaspersky business solutions

Configuring Kaspersky applications

- Scenario: Configuring network protection
- About device-centric and user-centric security management approaches
- Policy setup and propagation: Device-centric approach
- Policy setup and propagation: User-centric approach
- Policies and policy profiles
- About policies and policy profiles
- About lock and locked settings
- Inheritance of policies and policy profiles
- Hierarchy of policies
- Policy profiles in a hierarchy of policies
- How settings are implemented on a managed device
- Managing policies
- Viewing the list of policies
- Creating a new policy
- General policy settings
- Modifying a policy
- Enabling and disabling a policy inheritance option
- Copying a policy
- Moving a policy
- Exporting a policy
- Importing a policy
- Forced synchronization
- Viewing the policy distribution status chart
- Activating a policy automatically at the Virus outbreak event
- Deleting a policy

- Managing policy profiles
  - Viewing the profiles of a policy
  - Changing a policy profile priority
  - Creating a policy profile
  - Copying a policy profile
  - Creating a policy profile activation rule
  - Deleting a policy profile
  - Exporting and importing a policy profile
- Network Agent policy settings
- Usage of Network Agent for Windows, Linux, and macOS: Comparison
- Comparison of Network Agent settings by operating systems
- Enabling and disabling the low resource consumption mode for Network Agent
- Configuring protection settings of managed applications
- Manual setup of the group update task for Kaspersky Endpoint Security
- Manual setup of the group task for scanning a device with Kaspersky Endpoint Security
- Kaspersky Security Network (KSN)
  - About KSN
  - Setting up access to KSN
  - Enabling and disabling the usage of KSN
  - Viewing the accepted KSN Statement
  - Accepting an updated KSN Statement
  - Checking whether the distribution point works as KSN proxy server
  - Viewing the statistics of KSN proxy server
- Managing tasks
  - About tasks
  - About task scope
  - Creating a task
  - Starting a task manually
  - Starting a task for selected devices
  - Viewing the task list
  - General task settings
  - Exporting a task
  - Importing a task
  - Starting the Change tasks password wizard
    - Step 1. Specifying credentials
    - Step 2. Selecting an action to take
    - Step 3. Viewing the results
  - Viewing task run results stored on the Administration Server
- Application tags
  - Application tags
  - Creating an application tag
  - Renaming an application tag
  - Assigning tags to an application
  - Removing assigned tags from an application
  - Deleting an application tag
- Using the klscflag utility to open port 13291
- Registering Kaspersky Industrial CyberSecurity for Networks application in Kaspersky Security Center Web Console

Managing users and user roles
About user accounts
About user roles
Configuring access rights to application features. Role-based access control
Access rights to application features
Predefined user roles
Assigning access rights to specific objects
Assigning access rights to users and security groups
Adding an account of an internal user
Creating a security group
Editing an account of an internal user
Editing a security group
Assigning a role to a user or a security group
Adding user accounts to an internal security group
Assigning a user as a device owner
Assigning a user as a device owner during installation of Network Agent
Assigning a user as a Linux device owner after installation of Network Agent
Removing a user as a device owner
Enabling account protection from unauthorized modification
Configuring two-factor authentication
About two-factor authentication for an account
Configuring a two-factor authentication secret key at Kaspersky Security Center Web Console sign-in
Allowing users to configure two-factor authentication
Resetting and deleting a two-factor authentication secret key
Excluding accounts from two-factor authentication
Editing the name of a security code issuer
Changing the number of allowed password entry attempts
Deleting a user or a security group
Changing a user account password
Creating a user role
Editing a user role
Editing the scope of a user role
Deleting a user role
Associating policy profiles with roles
Propagating user roles to secondary Administration Servers
Changing account password
Revoking local administrator rights
Configuring Kerberos domain authentication
Updating Kaspersky databases and applications
Scenario: Regular updating Kaspersky databases and applications
About updating Kaspersky databases, software modules, and applications
Creating the Download updates to the Administration Server repository task
Verifying downloaded updates
Creating the task for downloading updates to the repositories of distribution points
Adding sources of updates for the Download updates to the Administration Server repository task
Approving and declining software updates
Automatic installation of updates for Kaspersky Endpoint Security for Windows

- About using diff files for updating Kaspersky databases and software modules
- Enabling the Downloading diff files feature
- Downloading updates by distribution points
- Updating Kaspersky databases and software modules on offline devices

Monitoring, reporting, and audit

- Scenario: Monitoring and reporting
- About types of monitoring and reporting
- Triggering of rules in Smart Training mode
  - Viewing and confirming detections performed using Adaptive Anomaly Control rules
  - Adding exclusions from the Adaptive Anomaly Control rules
- Dashboard and widgets
  - Using the dashboard
  - Adding widgets to the dashboard
  - Hiding a widget from the dashboard
  - Moving a widget on the dashboard
  - Changing the widget size or appearance
  - Changing widget settings
  - About the Dashboard-only mode
  - Configuring the Dashboard-only mode
- Administration and protection reports
  - Using reports
  - Creating report template
  - Viewing and editing report template properties
  - Exporting a report to a file
  - Generating and viewing a report
  - Creating a report delivery task
  - Deleting report templates
- Hardening center
  - Security application installed
  - Policy applied
  - Anti-virus databases update configured
  - Backup configured
  - Administration Server maintenance configured
  - TLS encryption enabled
  - All devices are managed
- Events and event selections
  - About events in Kaspersky Security Center Linux
  - Events of Kaspersky Security Center Linux components
    - Data structure of event type description
    - Administration Server events
      - Administration Server critical events
      - Administration Server functional failure events
      - Administration Server warning events
      - Administration Server informational events

Network Agent events
Network Agent functional failure events
Network Agent warning events
Network Agent informational events
Using event selections
Creating an event selection
Editing an event selection
Viewing a list of an event selection
Exporting an event selection
Importing an event selection
Viewing event detail areas
Exporting events to a file
Viewing an object history from an event
Deleting events
Deleting event selections
Setting the storage term for an event
Blocking frequent events
About blocking frequent events
Managing frequent events blocking
Removing blocking of frequent events
Event processing and storage on the Administration Server
Notifications and device statuses
About notifications
Viewing attention-required notifications
Viewing system notifications
Viewing announcements
Disabling Kaspersky announcements
Configuring the switching of device statuses
Configuring notification delivery
Testing notifications
About device statuses
Parameters and environment variables for describing an event
Viewing information about the detects of threats
Integrations for responding to alerts
Configuring integration with Active Directory for performing response actions
Configuring integration with Kaspersky Automated Security Awareness Platform
Configuring integration with Kaspersky Threat Intelligence Portal Sandbox
Grouping alerts by attributes
Cloud Discovery
Enabling Cloud Discovery by using the widget
Adding the Cloud Discovery widget to the dashboard
Viewing information about the use of cloud services
Risk level of a cloud service
Blocking access to unwanted cloud services
Export of events to SIEM systems
Configuring event export to SIEM systems
Prerequisites

About event export
About configuring event export in a SIEM system
About exporting events using CEF and LEEF formats
Converting events to the CEF or LEEF format
Marking of events for export to SIEM systems in Syslog format
Marking events of a Kaspersky application for export in the Syslog format
Marking general events for export in Syslog format
About exporting events using Syslog format
Configuring Kaspersky Security Center Linux for export of events to a SIEM system
Monitoring of policy and policy profile changes
Exporting events directly from the database
Executing an SQL query by using the klsql2 utility
Example of an SQL query in the klsql2 utility
Viewing the Kaspersky Security Center Linux database name
Viewing export results
Managing object revisions
Viewing and saving a policy revision
Comparing policy revisions
Rolling back an object to a previous revision
Active threats
Disinfecting an unprocessed file
Downloading an unprocessed file
Deleting files from the Active threats section
Deletion of objects
Downloading and deleting files from Quarantine and File backups
Downloading files from Quarantine and File backups
About removing objects from the Quarantine, File backups, or Active threats repositories
Managing the application over SNMP
Configuring the snmpd service in the operating system
Enabling and disabling notifying by SNMP
Enabling and disabling SNMP in Kaspersky Security Center Linux
Values of object identifiers for SNMP
Working with Kaspersky Security Center Linux under Kaspersky Next XDR Optimum license
Integrations for responding to alerts
Configuring integration with Active Directory for performing response actions
Configuring integration with Kaspersky Automated Security Awareness Platform
Configuring integration with Kaspersky Threat Intelligence Portal Sandbox
Grouping alerts by attributes
Integration between Kaspersky Security Center Web Console and other Kaspersky solutions
Establishing a background connection
Configuring proxy server connection
Remote diagnostics of client devices
Opening the remote diagnostics window
Enabling and disabling tracing for applications
Downloading trace files of an application
Deleting trace files
Downloading application settings

Downloading system information from a client device
Downloading event logs
Starting, stopping, restarting the application
Running the remote diagnostics of Kaspersky Security Center Linux Network Agent and downloading the results
Running an application on a client device
Running remote diagnostics on a Linux-based client device
Managing third-party applications and executable files on client devices
Using Application Control to manage executable files
Obtaining and viewing a list of executable files stored on client devices
Creating an application category with content added manually
Creating an application category that includes executable files from selected devices
Creating an application category that includes executable files from selected folder
Viewing the list of application categories
Adding event-related executable files to the application category
Configuring Application Control in the Kaspersky Endpoint Security for Windows policy
Obtaining and viewing a list of applications installed on client devices
About third-party applications
Installing third-party software updates
Scenario: Updating third-party software
Third-party software updates installation options
Find vulnerabilities and required updates task settings
Creating the Find vulnerabilities and required updates task
Viewing information about available third-party software updates
Exporting the list of available software updates to a file
Approving and declining third-party software updates
Creating the Install required updates and fix vulnerabilities task
Adding rules for update installation
Settings of the Install required updates and fix vulnerabilities task specified after task creation
Updating third-party applications automatically
Fixing third-party software vulnerabilities
About finding and fixing software vulnerabilities
Scenario: Finding and fixing third-party software vulnerabilities
Fixing third-party software vulnerabilities
Creating the Fix vulnerabilities task
Selecting user fixes for vulnerabilities in third-party software
Viewing information about software vulnerabilities detected on all managed devices
Viewing information about software vulnerabilities detected on the selected managed device
Viewing statistics of vulnerabilities on managed devices
Exporting the list of software vulnerabilities to a file
Ignoring software vulnerabilities
Creating an installation package of a third-party application from the Kaspersky database
Viewing and modifying the settings of an installation package of a third-party application from the Kaspersky database
Settings of an installation package of a third-party application from the Kaspersky database
Fixing vulnerabilities in an isolated network
Scenario: Fixing third-party software vulnerabilities in an isolated network
About fixing third-party software vulnerabilities in an isolated network
Configuring the Administration Server with internet access to fix vulnerabilities in an isolated network

Configuring isolated Administration Servers to fix vulnerabilities in an isolated network
Transmitting patches and installing updates in an isolated network
Disabling transmission of patches and installation of updates in an isolated network
API Reference Guide
Best Practices for Service Providers
Planning Kaspersky Security Center Linux deployment
Providing internet access to Administration Server
Kaspersky Security Center Linux standard configuration
About distribution points
Hierarchy of Administration Servers
Virtual Administration Servers
Deployment and initial configuration
Recommendations on Administration Server installation
Creating accounts for the Administration Server services on a failover cluster
Selecting a DBMS
Specifying the address of the Administration Server
Maintaining idle connections
Deploying Network Agent and security applications
Configuring protection on a client organization's network
Manual setup of the Kaspersky Endpoint Security policy
Configuring the policy in the Advanced Threat Protection section
Configuring the policy in the Essential Threat Protection section
Configuring the policy in the General Settings section
Configuring the policy in the Event configuration section
Manual setup of the group update task for Kaspersky Endpoint Security
Manual setup of the group task for scanning a device with Kaspersky Endpoint Security
Scheduling the Find vulnerabilities and required updates task
Manual setup of the group task for updates installation and vulnerabilities fix
Building a structure of administration groups and assigning distribution points
Standard MSP client configuration: Single office
Standard MSP client configuration: Multiple small remote offices
Hierarchy of policies, using policy profiles
Hierarchy of policies
Policy profiles
Tasks
Device moving rules
Software categorization
Backup and restoration of Administration Server settings
A device with Administration Server is inoperable
The settings of Administration Server or the database are corrupted
About connection profiles for out-of-office users
About switching Network Agent to other Administration Servers
Creating a connection profile for out-of-office users

- Remote access to managed devices
  - Using the "Do not disconnect from the Administration Server" option to provide continuous connectivity between a managed device and the Administration Server
  - About checking the time of connection between a device and the Administration Server
  - About forced synchronization
- Sizing Guide
  - About this Guide
  - Limitations of Kaspersky Security Center Linux
  - Calculations for Administration Servers
    - Calculation of hardware resources for the Administration Server
      - Hardware requirements for the DBMS and the Administration Server
      - Calculation of database space
      - Calculation of disk space
    - Calculation of the number and configuration of Administration Servers
    - Recommendations for connecting dynamic virtual machines to Kaspersky Security Center
  - Calculations for distribution points and connection gateways
    - Requirements for a distribution point
    - Calculating the number and configuration of distribution points
    - Calculation of the number of connection gateways
  - Logging information about events for tasks and policies
  - Best practices for an Administration Server that manages a large number of devices
  - Specific considerations and optimal settings of certain tasks
    - Device discovery frequency
    - Administration Server data backup task and database maintenance task
    - Group tasks for updating Kaspersky Endpoint Security
    - Inventory task
  - Details of network load spread among Administration Server and protected devices
    - Traffic rate under various scenarios
    - Average traffic usage per 24 hours
- Known issues and limitations
- Contact Technical Support
  - How to get technical support
  - Technical support via Kaspersky CompanyAccount
  - Obtaining dump files of Administration Server
- Sources of information about the application
- Glossary
  - Active key
  - Administration Console
  - Administration Group
  - Administration Server
  - Administration Server certificate
  - Administration Server client (Client device)
  - Administrator rights
  - Administrator's workstation
  - Anti-virus databases
  - Anti-virus protection service provider
  - Anti-virus security of the network

Application settings
Application Shop
Authentication Agent
Available update
Backup copying of Administration Server data
Backup folder
Broadcast domain
Centralized application management
Client administrator
Cloud Discovery
Configuration profile
Connection gateway
Demilitarized zone (DMZ)
Device owner
Direct application management
Event repository
Event severity
FileTransferBridge
Group task
Home Administration Server
HTTPS
Identity and Access Manager (IAM)
Incompatible application
Installation package
Internal users
iOS MDM device
iOS MDM Server
JavaScript
Kaspersky Security Center Linux Administrator
Kaspersky Security Center Linux Web Server
Kaspersky Security Center Operator
Kaspersky Security Center System Health Validator (SHV)
Kaspersky update servers
Key file
License term
Lightweight Nagent (LWNGT)
Local installation
Local task
Managed devices
Manual installation
Network Agent
Network Location Awareness (NLA)
Network protection status
Patch importance level
Policy
Profile
Protection status

Provisioning profile
Remote installation
Reserve key
Restoration
Restoration of Administration Server data
Role group
Service provider's administrator
Shared certificate
SSL
Task
Task for specific devices
Task settings
Update Agent
Updating
Virtual Administration Server
Virus outbreak
Vulnerability
Information about third-party code
Trademark notices

# Kaspersky Security Center Linux Help

## New features

- What's new

## Hardware and software requirements

- Administration Server requirements
- Web Console requirements
- Network Agent requirements

## Getting started

- Installation
- Quick start wizard
- Protection deployment wizard

## Licensing and activation

- Activating Kaspersky Security Center Linux
- Licensing of managed applications

## Deployment and configuration

- Discovering networked devices
- Adjustment of distribution points and/or connection gateways
- Replacing third-party security applications
- Kaspersky application deployment Centralized deployment

- Configuring network protection
- Kaspersky application deployment Updating databases and software modules
- Configuring the Administration Server connection address
- Migration to Kaspersky Security Center Linux
- About upgrading Kaspersky Security Center Linux

## Monitoring

- Monitoring and reporting
- Cloud Discovery

## Managing client devices

- Remote access to managed devices

## Vulnerability and patch management

- Finding and fixing third-party software vulnerabilities

## Additional features

- Export of events to SIEM systems
- Viewing the statistics of KSN proxy server
- Sizing Guide (Online Help only)

# What's new

## Kaspersky Security Center 17 Linux

Kaspersky Security Center 17 Linux has several new features and improvements:

- Web Console, IAM and Administration Server certificates can now be added manually and automatically replaced without reinstalling the Web Console.
- When viewing the contents of a revision or comparing policy revisions, policy profile data is now available.
- Now, after running a task for a device or a specific devices, you can go to the task's properties to view the results.
- A new protection level indicator has been added to the Hardening center, allowing you to track devices over which control may have been lost.
- The following information about client devices has been added to events published by the Administration Server for managed devices: DNS name (FQDN), NetBIOS name, IP address, and DisplayName.
- Audit capabilities have been expanded:
  - When Network Agent switches over to another Administration Server, an event is now logged in the Kaspersky Event Log. The event indicates the address of the new Administration Server and the gateway address, if any.
  - Extended events are now sent when importing and copying policies, as well as when rolling back a policy to a selected revision.
- User experience improvements:
  - The **Tags** section has been renamed to **Device tags**.
  - The **Device tags** section with its subsections has been moved from the **Asset management** section to the **Repositories** section.
  - Now you can download all events for a device or a selection of events from the events list as a file.
- The quick installation script for Kaspersky Security Center Linux now supports additional deployment options:
  - MySQL 8.4.10 with Ubuntu Server 26.04 LTS
  - MariaDB 10.11.18 with CentOS Stream 10
  - MariaDB 10.11.18 with RED OS 8
  - MariaDB 10.11.13 with Astra Linux 1.8.5

- The Administration Server now supports new DBMS versions:
  - MariaDB 11.4
  - MariaDB 11.8
  - MariaDB 12.3
  - Platform V Pangolin 7.2.0
  - Platform V Pangolin 7.2.0 (Built-in High Availability cluster)
- The Administration Server and Web Console now support the following new versions of operating systems:
  - ALT Server 11
  - MosOS 15.6
- Network Agent now supports work with the following new operating system versions:
  - Microsoft Windows 11 26H2 Home/Pro/Pro for Workstations/Enterprise/Education
  - Microsoft Windows 10 IoT Enterprise version 1507
  - Debian GNU/Linux versions 12.10, 12.11, 12.14 (Bookworm) ARM
  - Astra Linux Special Edition RUSB.10015-16 (release 2) (operational update 8.1) E2K
  - Astra Linux Special Edition RUSB.10265-01 (operational update 8.1) E2K
  - Elbrus 9.3.6 E2K
  - ALT Workstation 11.2 ARM
  - ALT Server 11.1 ARM
  - ALT SP Workstation 10 E2K
  - ALT SP Server 10 E2K
  - ALT 8 SP Workstation E2K
  - ALT SP Server 8 E2K
  - MSVSPHERE 9.5 SERVER
  - MSVSPHERE 9.5 ARM
  - Amazon Linux 2023
  - MosOS 15.6

## Kaspersky Security Center 16.3 Linux

Kaspersky Security Center 16.3 Linux has several new features and improvements:

- If you modify a policy, a separate audit event is created for every parameter that was changed. The events are exported to SIEM.
- Support for **Kaspersky SIEM** (KUMA) is now added to the functionality of event export to SIEM systems.
- Kaspersky Security Center Linux now supports work with Kaspersky Vulnerability Management solution.
- For compliance with Hardening Guide, we worked out an optimized Kaspersky Endpoint Security for Linux configuration for installation on the devices with Administration Server, Web Console and DBMS as well as for deploying Kaspersky Security Center Linux failover cluster.
- You can now specify custom database schema while installing Kaspersky Security Center Linux.
- In **Monitoring** → **Dashboard**, the protection level indicator helps you evaluate the security of your Administration Server and distribution points. If the indicator is yellow or red, you have to perform actions to resolve issues and change the indicator state to green.
- A simplified method of Kaspersky Security Center Linux deployment is available. You can now use an installation script.
- A special distribution package for Kaspersky Network Agent for Linux Legacy with glibc version 2.5 is available to support the following outdated operating systems:
  - CentOS 5.2
  - CentOS 5.4
  - CentOS 6.4
  - CentOS 6.6
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.4) 64-bit
- Network Agent now supports work with the following new operating system versions:
  - Microsoft Windows 11 IoT Enterprise version 25H2 64-bit
  - SberOS 3.6.1
  - Ubuntu Server 26.04 LTS
- The following DBMSs are no longer supported:
  - MySQL 5.7
  - MariaDB 10.1.30

- User experience improvements:
  - Enhanced filtering for **Tasks** and **Policies** tables. You can now add multiple conditions by using `OR` logic; as well as use a new operator, which allows you to select multiple values for a single property and display records that match at least one of the specified criteria.
  - In the main menu:
    - A new **Software management** section is available. The following sections are now moved to **Software management**: **Installation packages**, **Kaspersky applications**, **Third-party applications**, **Kaspersky software catalog**, and **Patch management**.
    - The **Unassigned devices** and **Hardware** sections are now moved to the **Asset management**.
    - **Tasks** and **Repositories** sections are moved to the first level of the menu.
    - **Web plug-in backups** section is no longer used and removed from Web console.

## Kaspersky Security Center 16.2 Linux




Overview of new features in version 16.2. Video

Kaspersky Security Center 16.2 Linux has several new features and improvements:

- In Kaspersky Security Center Web Console, you can now configure a connection gateway in the demilitarized zone (DMZ).

  Use the **Use DMZ connection gateway by address** option for configuring a connection gateway.

- Improved the algorithm for preserving the Network Agent device identifier (the `Device ID` parameter) on Linux devices. If a device's BIOS serial number, motherboard serial number, storage disk identifiers, or MAC address match previously known values, Administration Server correctly identifies the device as previously discovered after an operating system update or a MAC address change.

- Added support for a geographically distributed Kaspersky Security Center Linux failover cluster with nodes located across different data centers. In the geo-distributed cluster configuration, all components are failover.

- You can now export events to a SIEM system, in the CEF or LEEF formats.

- Added support for the high-availability PostgreSQL cluster with Patroni for automated failover and HAProxy for load balancing.
- You can compare policy revisions. The option is available for the policies of Administration Server, Network Agent, Kaspersky Endpoint Security for Windows (starting from 14.0 web plug-in version), and Kaspersky Endpoint Security for Mac (starting from 12.2.1 Patch A web plug-in version). The list of Kaspersky applications that support this feature will be expanded in future versions.
- SNMP is now supported. You can provide Administration Server information, statistics, and events to third-party client applications by using SNMP.
- Windows network polling is now supported for Windows-based distribution points.
- A single installation package for Network Agent for Linux is now available. This installation package includes versions for different package managers and CPU architectures. During installation, the environment is automatically detected and the appropriate Network Agent package is installed.
- Events now include information about the initiator of commands executed on mobile devices.
- The NSQ component is removed from the Kaspersky Security Center Web Console distribution package. The service KSCWebConsoleMessageQueue.service is no longer used and will be removed after the Kaspersky Security Center Web Console update.
- If the Administration Server does not have access to the repository of application distributions for remote installation, then before creating installation packages from a file for applications on Windows devices, you need to download additional modules from the Kaspersky website: Files for remote installation via Kaspersky Security Center (the ri_utils_win32.zip and ri_utils_arm64.zip archives).
- Network Agent now supports the Windows ARM 64-bit architecture. Compatibility with managed applications can be verified in the corresponding Help documentation.
- Kaspersky Security Center Linux supports work with Kaspersky Sandbox.
- User experience improvements:
  - You can now delete all events from an event selection and from a device event list at once.

    The **Select all** and **Select all on current page** options are available in the event selection and in the device event list.
  - You can now manually specify a moving rule priority.

    The **Change priority** button becomes available when you select a moving rule and allows you to specify the new priority.
- Kaspersky Security Center Linux supports work with Platform V SberLinux OS Server (SLO) 9.6.
- Kaspersky Security Center Linux now supports work with the following DBMSs:
  - MySQL Standard Edition 8.4
  - MySQL Enterprise Edition 8.4
  - PostgreSQL 18

- Postgres Pro 18 (all editions)
- Postgres Pro 18 Enterprise (cluster Built-in High Availability)

- Network Agent now supports work with the following new operating system versions:
  - Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM
  - Platform V SberLinux OS Server (SLO) 9.6

## Kaspersky Security Center 16.1 Linux

Kaspersky Security Center 16.1 Linux has several new features and improvements:

- Two-factor authentication is now enabled by default. The global option to disable two-factor authentication is no longer available. To ensure that users can sign in to Kaspersky Security Center Web Console and continue using OpenAPI automation scripts, enable two-factor authentication for all users before the upgrade.
- You can now save a policy profile to a KLPROF file without exporting a policy, and then use this KLPROF file to import the saved profile to the policy.
- Network Agent now operates on a device running ALT OS in the closed software environment mode.
- Added support for Kerberos-based domain authentication for passwordless domain users by using the SCRIL protocol, enabling certificate-based single sign-on (SSO).
- User experience improvements:
  - Filtering of client devices by operating system version and package manager now includes Linux operating system versions.
  - Improved the pagination mechanism for tables in Kaspersky Security Center Web Console: the default number of displayed items has been increased to 50, and the custom number of displayed items is now preserved between sessions.
  - Comments for application categories that allow you to add descriptions of rules for including and excluding applications within a category.
  - By default, the list of available installation packages now displays only Kaspersky application installation packages in the Kaspersky Security Center Web Console interface language and in English.
- Kaspersky Security Center Linux supports work with Kaspersky Endpoint Security for Linux 12.4.
- Kaspersky Security Center Linux supports work with the following new operating system versions:
  - Debian GNU/Linux 13 (Trixie)
  - CentOS Stream 10
  - Red Hat Enterprise Linux Server 10.x

- Network Agent now supports work with the following new operating system versions:
  - ALT Workstation 11
  - ALT Server 11
  - ALT Education 11
  - AlterOS 2025
  - SberOS 3.4.0
  - SberOS 3.5.0
  - OSnova 3.*

## Kaspersky Security Center 16 Linux

Kaspersky Security Center 16 Linux has several new features and improvements:

- FreeIPA and ALD Pro domain controllers are supported.
- Domain authentication (single sign-on) is implemented. The single sign-on feature allows you to enable secure authentication in Kaspersky Security Center 16 Web Console without re-entering the password on the corporate network. To use domain authentication, you must specify the additional parameters in the response file during Kaspersky Security Center Web Console installation.
- Kaspersky Security Center 16 Linux Administration Server is only compatible with Kaspersky Security Center 16 Web Console. Earlier versions of Kaspersky Security Center Web Console cannot be used.
- You can now use the Kaspersky Next XDR Optimum functionality under a trial license provided that you added a secondary Administration Server, activated this server under the trial license, and deployed the license key to the devices managed by the secondary Administration Server.
- User experience improvements:
  - Navigation through the administration groups and Administration Servers is updated: you can easily switch between groups and Servers from a single navigation pane.
  - Your profile settings are moved to the upper pane.
  - The following sections of the main menu are renamed:
    - **Assets (Devices)** section is now called **Asset management**.
    - **Managed devices** is called **Managed devices**.
    - **Quick links** is renamed to **Console navigation**.
  - You can minimize the main menu to icons, if necessary.
  - The **Kaspersky news** section is deleted from **Monitoring** → **Notifications**.

- The filters that you apply to tables in the **Operations** → **Patch management** → **Software vulnerabilities** and **Operations** → **Patch management** → **Software updates** sections are now successfully saved and not reset.
- Kaspersky Security Center Linux supports work:
  - With Kaspersky NGFW
  - With the following operating system versions (for the managed devices):
    - MosOS 15.5 Arbat
    - Microsoft Windows 11 25H2
    - CentOS 6.4
    - CentOS 6.6

## Kaspersky Security Center 15.4 Linux

Kaspersky Security Center 15.4 Linux has several new features and improvements:

- Connection profiles for out-of-office users with Linux devices are now available. By using connection profiles, you can configure the rules for Network Agents on Linux devices to connect to the same or different Administration Servers, depending on the device location.
- Transmitting encryption keys between Administration Servers is now available.
- Kaspersky Thin Client is now supported.
- The Platform V Pangolin Built-in High Availability cluster is now supported.
- The Postgres Pro Built-in High Availability cluster is now supported. The nodes of this DBMS cluster are specified in the connection string when installing Kaspersky Security Center Linux.
- Kaspersky Security Center Linux now supports work with the following DBMSs:
  - Platform V Pangolin 6.5.1
  - Tantor SE 1C for Astra Linux Special Edition RUSB.10015-01 (operational update 1.8)
  - Jatoba 5
- Support for Platform V SberLinux OS Server (SLO) versions 8.10.1, 9.0.1, 9.5.1.
- The KlAkOAPI.tar.gz archive is deleted from Help. The KlAkOAPI.tar.gz archive is located in the Kaspersky Security Center Linux installation folder.
- The **Scan** button is deleted from the **Quarantine** section.
- Information about the size, file hash, and path is no longer available in the list of installation packages for the Network Agent stand-alone package or for any packages created on virtual Administration Servers, because these standalone packages are generated at the time of download.

*Kaspersky Security Center 15.4 Linux under Kaspersky Next XDR Optimum license*

If you activated Administration Server under Kaspersky Next XDR Optimum license and deployed the Kaspersky Next XDR Optimum license key to your managed applications, you can do the following:

- Group alerts by attributes.
- Configure integrations for responding to threats.

## Kaspersky Security Center 15.3 Linux

Kaspersky Security Center 15.3 Linux has several new features and improvements:

- The klcsngtgui utility is removed from the Kaspersky Security Center Linux distribution kit. We recommend using the klnagchk utility instead of the klcsngtgui utility.
- Network Agent now supports work with the following new operating system versions:
  - Windows Server 2025
  - Fedora Linux Server 41
  - Fedora Linux Workstation 41
- Kaspersky Security Center Linux now supports work with the following DBMSs:
  - PostgreSQL 17
  - Postgres Pro 17
- You can now download only the required updates of databases and software modules for Kaspersky security applications by using Kaspersky Update Utility. In the **Download updates to the Administration Server repository** task properties window, enable the **Download the update request file automatically** option, and then specify the path where Kaspersky Security Center Linux will create the update request file with information about the updates to be downloaded.
- Viewing usage statistics of KSN proxy server is now available.
- Migrating the Kaspersky Security Center Windows Administration Server data to Kaspersky Security Center Linux by using the klbackup utility has been updated. Now, you can migrate Administration Server data stored in the Microsoft SQL Server database to PostgreSQL or Postgres Pro.
- Configuring the Administration Server connection address is now available. The Administration Server connection address is used as a default address when creating the Network Agent installation packages and as the KSN proxy server address when connecting managed devices to KSN.
- You can now centrally restart managed devices.
- Information about the users currently logged in to the Linux managed device is now displayed in the **General** → **Sessions** section of the device properties window.

- You can now obtain remote access to the Linux and Windows managed devices through Network Agent installed on these devices. Connection is established by using RDP, VNC, or WDS. Upon establishing a connection with the device, the administrator gains full access to information stored on this device and can manage applications installed on it.

- Upload and run an application (or script) for diagnostics on a managed device. You can now upload either the directory or archive containing the executable file, or the executable file itself. After the application is successfully executed, you can download the execution results.

- User experience improvements, including a new **Quick links** section. This section displays the main menu map and provides you quick access to all sections of Kaspersky Security Center Web Console. By default, **Quick links** is set as the home page.

## Kaspersky Security Center 15.2 Linux

Kaspersky Security Center 15.2 Linux has several new features and improvements:

- New features for managing passwords of internal user accounts:

  - You can now force an internal user to change a password at the first (or next) attempt to sign in to Kaspersky Security Center Web Console.

  - New option to configure the password expiration period for internal user accounts.

- You can now back up the Kaspersky Security Center Windows Administration Server data and restore it in Kaspersky Security Center Linux by using the klbackup utility. Migration can be performed without data loss between DBMS of the same type, or Microsoft SQL Server → MySQL or MariaDB.

- Kaspersky Security Center Linux now supports work with the following DBMSs:

  - PostgreSQL 16.x

  - Postgres Pro 16.x

- Kaspersky Security Center Linux now supports some types of PostgreSQL and Postgres Pro clusters.

- Support for new operating systems and new operating system versions, including new versions of OS MES (Moscow Electronic School), MosTech, and MosTech Server.

- User experience improvements, including:

  - New **Save** button in the policy settings window. Use this button if you want to save the changes without closing the policy settings window.

- You can now manage sending files to Android devices, delete the previously sent files, and configure their settings in the new "Apps & files" section of the Kaspersky Mobile Devices Protection and Management plug-in.

- You can now transfer app installation packages and device management profiles to mobile devices without directly connecting them to the Administration Server using a new Web Server service on a connection gateway.

## Kaspersky Security Center 15.1 Linux

Kaspersky Security Center 15.1 Linux has several new features and improvements:

- Kaspersky Security Center Web Console now supports mobile device management via the Kaspersky Mobile Devices Protection and Management plug-in.
- You can now install and configure iOS MDM Servers via the iOS MDM Server settings plug-in to manage iOS MDM devices.
- You can now manage the certificates of mobile devices.
- Kaspersky Endpoint Security for Android is now supported.
- Kaspersky Security for iOS is now supported.
- Kaspersky Endpoint Security for Aurora is now supported.
- Vulnerability and patch management for Windows-based managed devices. You can manage the updates of third-party software installed on Windows-based managed devices and fix vulnerabilities in such software through the installation of required updates.
- Kaspersky Security Center Linux now polls domain controllers page by page instead of polling the entire domain controller at once. This allows you to poll domain controllers that include a large number of entries.
- Adaptive Anomaly Control. This is a Kaspersky Endpoint Security for Windows feature that uses a set of rules to track non-typical behavior on client devices and allows you to block anomalous actions.
- Seamless updates for managed Kaspersky applications installed on Windows devices and Network Agent for Linux. You can manage the update installation process by approving updates that must be installed and declining updates that must not be installed.
- Extended policy audit. You can now view the contents of a policy revision and save a policy revision to a file. Currently, these features are only available for the Administration Server policy and Network Agent policy.
- Cloud Discovery. This is a new feature that allows you to monitor the use of cloud services on managed devices running Windows and to block access to cloud services that you consider unwanted.
- New **Alerts** subsection in the **Monitoring** section of the main menu. In the **Alerts** subsection, you can view information about the detects of threats on the endpoint devices. The threats are detected by Kaspersky security applications.
- Kaspersky Security Center Linux can now act as a component of the Kaspersky Managed Detection and Response solution.
- Support for Kaspersky Security for Virtualization Light Agent.
- Extended hardware inventory of macOS devices. Network Agent on a macOS device sends the MAC address and device serial number to Administration Server.
- You can now receive a report on remote installation when you install software on the managed devices through custom scripts.

- When you execute several custom scripts on a managed device, you can set a priority for each script to define the execution order. The scripts will be executed from the one with the highest priority to the one with the lowest priority.

- To reduce the amount of RAM consumed by Kaspersky Endpoint Security for Linux and Network Agent for Linux, you can enable a special work mode for Network Agent for Linux. In this mode, Network Agent for Linux requires less RAM, but its functionality is limited.

- You can uninstall incompatible software from the managed devices through the *Uninstall application remotely* task.

- Report on network attacks now includes the MAC address and port of the attacking device.

- The maximum password length for an internal user was increased to 256 characters.

- User experience improvements, including:

  - Main menu personalization by adding sections of Kaspersky Security Center Web Console to bookmarks for quick access from the **Bookmarks** section.

  - Optimized work with tables. The default view of each table now contains the most frequently used columns. Also, you can now select all items on the current page or in the entire table, as well as sort items in the entire table.

  - Improved report delivery configuration. You can now specify up to 20 email addresses to send the report to, and the report delivery schedule.

- Support for a wide range of operating systems and new operating system versions.

- A new sizing guide was developed and published in the Online Help.

- As a result of a user interface review, an issue that led to the **Remote diagnostics** section appearing in the Administration Server properties window was resolved.

- You can create an *Execute scripts remotely* task to execute an installation package on a client device and to install an application remotely.

- A user can be assigned as a device owner during or after installation of Network Agent on a client device on Linux.

- You can configure a device selection or create a device moving rule based on a device owner, device owner's membership in a security group, and device owner's role.

- You can revoke local administrator rights from accounts. This provides you with an extra layer of control of user accounts. For example, you can revoke local administrator rights after a one-time assignment is complete.

- You can change the local account password, for example, when the user forgets the local account password or to perform a scheduled password change.

- In the **User certificates management** subsection, you can specify which root certificates to install. These certificates can be used, for example, to verify the authenticity of websites or web servers.

## Kaspersky Security Center 15 Linux

Kaspersky Security Center 15 Linux has several new features and improvements:

- Domain controller polling allows you to poll a Microsoft Active Directory domain controller and a Samba domain controller. You can use Administration Server or a distribution point to poll Microsoft Active Directory. You can poll a Samba domain controller only through a Linux-based distribution point. When you poll a domain controller, Administration Server or a distribution point retrieves information about the domain structure, user accounts, security groups, and DNS names of the devices that are included in the domain.
- Kaspersky Security Center Linux now supports work with the following DBMSs:
  - PostgreSQL 15.x
  - Postgres Pro 15.x
- If you use PostgreSQL or Postgres Pro as a DBMS, Kaspersky Security Center Linux supports up to 50,000 managed devices.
- Migration from Kaspersky Security Center Windows to Kaspersky Security Center Linux. You can run a wizard to migrate Kaspersky Security Center objects, including tasks, policies, and administration group structure. After that, you can move the imported managed devices to be under management of Kaspersky Security Center Linux.
- Kaspersky Security Center Linux now supports work with the following Kaspersky applications:
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Embedded Systems Security for Windows
  - Kaspersky Embedded Systems Security for Linux
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Networks
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Security for Virtualization Light Agent
- Remote diagnostics of Windows-based and Linux-based managed devices.
- Improved Application Control component. You can now create an application category based on the list of executable files from a selected folder or based on a Kaspersky application category. Then you can specify whether you want to allow or block the applications from the created category in your organization.
- Export and import of event selections. You can export a user-defined event selection and its settings to a KLO file, and then import the saved event selection to Kaspersky Security Center Windows or Kaspersky Security Center Linux.
- In the Report on threats, you can now open a threat development chain by clicking the **View alert** link.

- Kaspersky Security Center Linux now supports cluster technology. If an administration group contains clusters or server arrays, the **Managed devices** page displays two tabs—one for individual devices, and one for clusters and server arrays. After the managed devices are detected as cluster nodes, the cluster is added as an individual object to the **Clusters and server arrays** tab. The cluster nodes are listed on the **Devices** tab, along with other managed devices.

- Support for some platforms by Kaspersky Security Center Linux has ended because these platforms are no longer supported by their vendors.

## Kaspersky Security Center 14.2 Linux

Kaspersky Security Center 14.2 Linux has several new features and improvements:

- In an Administration Server hierarchy, a Linux-based Administration Server can now act as a primary Server and can manage Linux-based or Windows-based Servers acting as a secondary one.

- Kaspersky Security Center Linux now supports Kaspersky Security Network (KSN), KSN Proxy service, and Kaspersky Private Security Network (KPSN).

- Kaspersky Security Center Linux now supports Kaspersky Endpoint Security for Windows as a managed application.

  Remote installation of Network Agent for Windows on client devices is possible only by using operating system tools through Windows-based distribution points.

- Data on Windows-based managed devices can now be encrypted to reduce the risk of unintentional leakage of sensitive and corporate data if a laptop or hard drive is stolen or lost. This feature is implemented through Kaspersky Endpoint Security for Windows.

- Kaspersky Security Center Linux allows you to download and update both distribution packages of Kaspersky applications and management web plug-ins right in the user interface of Kaspersky Security Center Linux.

- By default, information about applications installed on the Linux-based and Windows-based managed devices is sent to Administration Server.

- Access to Kaspersky servers is now verified automatically. If access to the servers by using the system DNS is not possible, the application uses the public DNS.

- Sensitive data that is transferred between the primary Administration Server, secondary Administration Servers, and Network Agents is now protected with the AES encryption algorithm.

- User rights on a virtual Administration Server are available for configuration any time, independently from the primary Administration Server. Also, you can assign primary Server users the rights to manage a virtual Server.

- Kaspersky Security Center Linux now supports work with the following DBMSs:

  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (all editions)
  - Postgres Pro 14.x (all editions)

- You can use Kaspersky Security Center Web Console to export policies and tasks to a file, and then import the policies and tasks to Kaspersky Security Center Windows or Kaspersky Security Center Linux.
- The **Do not use proxy server** option has been removed from the following tasks:
  - *Download updates to the Administration Server repository*
  - *Download updates to the repositories of distribution points*

## Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux has several new features and improvements:

- Besides the *Download updates to the Administration Server repository* task, anti-virus databases for Kaspersky security applications can now be downloaded through the *Download updates to the repositories of distribution points* task.
- Anti-virus databases and application modules on the managed devices can be propagated and updated through Administration Server or distribution points. You can choose an update scheme optimal for your organization, to reduce the load on Administration Server and optimize data traffic on the corporate network.
- Kaspersky Security Center Linux downloads from Kaspersky update servers only those updates that are requested by the Kaspersky security applications. This reduces the size of the downloaded data.
- You can now use the diff files feature to download anti-virus databases and software modules. A diff file describes the differences between two versions of a file of a database or software module. The usage of diff files saves traffic inside your company's network because diff files occupy less space than entire files of databases and software modules.
- The *Update verification* task was added. By using this task, you can automatically check the downloaded updates for operability and errors before you install the updates on the managed devices.
- Kaspersky Security Center Linux now supports Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 as a managed application.

# Fixed issues

The table below lists all issues found in previous Kaspersky Security Center Linux versions, and which are fixed in the current version.

## List of issues fixed in Kaspersky Security Center Linux 17

| Kaspersky Security Center Linux version the issue first appeared in | Issue ID | Issue description |
|---|---|---|
| 16.2 | 10575601 | Fixed the issue that prevented the list of groups from being displayed in the drop-down list when the **Device is located in a subgroup of the Domains group** setting was enabled. |
| 16.3 | 10519188 | Fixed an issue where vacuuming (`VACUUM`) temporary tables slowed down the Administration Server. |
| 16.3 | 10530831 | Fixed the issue whereby changes in the **Managed devices** section were not saved after changing the order of columns. |
| 16.3 | 10698217 | Fixed the issue whereby in the properties of a managed device, on the **Advanced** → **Remote diagnostics** → **Event logs** tab, when clicking the **Remote installation logs** link, the displayed window was titled **Device tracing logs**. |
| 16.3 | 10696918 | Fixed the issue whereby the search window would not open on the secondary Server in the **Third-party applications** → **Application categories** section when navigating to the category properties on the **Conditions** tab. |
| 16.3 | 10720529 | Fixed the issue whereby the data was displayed incorrectly in the table of managed devices in the **Last connected to Administration Server** filter when using the "≠" (not equal) operator. |
| 16.3 | 10012561 | Fixed the issue whereby scanning a domain using SberLDAP would not return the structure of the domain and its hosts. |
| 16 | 9496192 | Fixed the issue whereby clicking the **Select all** button in the **Event selection** table and then exporting them would export events from the current page only. |
| 16.3 | 10292104 | Fixed the issue whereby in Kaspersky Security Center Web Console version 15.1 or 15.2, if you updated Kaspersky Endpoint Detection and Response Optimum plug-in to version 16.3, the **Alerts** section might not display alerts. |
| 16.3 | 10596319 | Fixed the issue whereby in the **Tags** section of the **Assign tag** form, the list of tags was displayed unsorted. |
| 16.3 | 10127434 | Fixed the issue whereby when you logged in to the Kaspersky Security Center Web Console and navigated to the **Tasks** section on the primary Administration Server, the virtual Administration Server was displayed as the primary Server in the hierarchy window. |
| 16.3 | 10252324 | Fixed the issue whereby some applications from the event selection generated by the **App Control** component in the Kaspersky Endpoint Security policy would not be added to the **Application categories** section. |
| 16.3 | 10308380 | Fixed the issue whereby after creating an application category, its properties would not open. |
| 16.2 | 10698205 | Fixed an issue whereby the **Clusters and server arrays** section would not display when selecting a cluster in the **Managed devices** section, which made it impossible to move a cluster to a group. |
| 16.3 | 10373324 | Fixed the issue whereby the second cluster node of a Kaspersky Security Center Linux failover cluster was not taken into account when evaluating the security indicator status. |
| 16.3 | 10563031 | Fixed the issue that caused an error while upgrading the Kaspersky Security Center Linux failover cluster from version 16.2 to version 16.3 and from version 16 to version 16.3. The error was "Attempt to change KLFOC-mode in upgrade. Aborting". |
| 16.3 | 10590796, 10590805 | Fixed the issue whereby upgrading the secondary node of the Kaspersky Security Center failover cluster resulted in errors: "Fatal error: It is forbidden to change KLFOC-management mode!" and "Fatal error: Can't get KSC DB name from settings storage." |

| | | |
|---|---|---|
| 16.3 | 10570574 | Fixed the issue whereby restarting the Administration Server service while the **Backup of Administration Server data** task was running resulted in the task restarting with an "Backup is already in progress" error. |
| 16.3 | 10085767 | Fixed the issue whereby the scope of the report might be displayed incorrectly when migrating data to Kaspersky Security Center Linux. |
| 16.2 | 10135898 | Fixed the issue whereby the **Settings** → **Single sign-on** section would not load if the user session lasted more than one hour. |
| 16.3 | 10542356 | Fixed the erroneous validation of the **Email address** field when editing a user in the **Users & roles** → **Users & groups** section. |
| 16.3 | 10534809 | Fixed the issue where events of a managed device took a long time to load. Load time reduced from 20 seconds to 2 seconds. |
| 16.3 | 10537996 | Fixed the issue whereby a browser tab with Kaspersky Security Center Web Console consumed more than 1.5 GB of RAM. |
| 15.1 | 9067495 | Fixed the issue whereby the **Check connection** button was available when saving the SIEM connection settings with the UDP protocol. |

## List of issues fixed in Kaspersky Security Center Linux 16.3 Update 1

| Kaspersky Security Center Linux version the issue first appeared in | Issue ID | Issue description |
|---|---|---|
| 16.3 | 10431901 | Fixed an issue that caused the **Single sign-on** section to be missing from the Web Console menu. Because of this, users could not configure domain authentication using the Kerberos protocol. Previously configured authentication continued to work. |

## List of issues fixed in Kaspersky Security Center Linux 16.3

| Kaspersky Security Center Linux version the issue first appeared in | Issue ID | Issue description |
|---|---|---|
| 16.2 | 9959974 | Fixed the issue that made the **Select all** option appear on the **Events** tab of the device properties window, which could result in deleting all events from the Administration Server database if it were to be selected. |
| 16.2 | 9392997 | Fixed the issue that caused an error message to be logged after successfully polling an ALD Pro or FreeIPA domain controller. |
| 16.2 | 9504495 | Fixed an issue that might cause an incorrect assignment of a user is a device owner is assigned via Network Agent installation package parameters. |
| 16.1 | 9316206 | Fixed an issue where control buttons might disappear from the **Two-factor authentication** tab when refreshing the browser after you open the tab. |
| 16.1 | 7555541 | Fixed an issue that caused a failure to sign in to Web Console if you enable the **Set as a one-time password (the user must change the password after the first login)** option when creating the *Change account password (Linux only)* task. |
| 15.4 | 7555788 | Fixed an issue when the *Change account password* task might not work correctly if SELinux was enabled on the user device. |
| 16.2 | 9603496 | Fixed an issue where you had to install Network Agent on the Administration Server device to obtain diagnostic information about this device. |
| 16.2 | 9704308 | Fixed an issue where opening the **Hierarchy of groups** section during page loading in environments with a large number of administration groups could result in a `429 Too Many Requests` error, interrupt the connection to the Administration Server, and redirect users to the sign-in page. |
| 16.2 | 9989231 | Fixed an issue where filtering devices by connection IP address could return incorrect results. |

| | | |
|---|---|---|
| 16.2 | 9990025 | Fixed an issue where table view settings in the **Policies** and **Tasks** sections were not preserved when navigating between pages. |
| 15.3 | 9632613 | Fixed an issue where domain user sign-in to the Web Console could be significantly delayed when LDAP domain controllers were unavailable or did not contain the user account. |
| 15.1 | 9829027 | Fixed an issue where configuring the **Update status** filter in the **Report on usage of anti-virus databases** report could result in an error. |
| 15.1 | 9844707 | Kaspersky Security Center and FCM (Firebase Cloud Messaging) interacted directly, even if a proxy server was configured. |

## List of issues fixed in Kaspersky Security Center Linux 16.2

| Kaspersky Security Center Linux version the issue first appeared in | Issue ID | Issue description |
|---|---|---|
| 15.1 | 10071566 | Fixed an issue where changes made to a task schedule were not propagated to managed devices if the schedule used the "By days of week" setting. |
| 15.4 | 9067754 | Fixed an issue that caused new events to display incorrectly in a previously created policy after updating the Kaspersky Mobile Devices Protection and Management plug-in. |
| 16 | 9329729 | Fixed an issue where an error appeared in the Kaspersky Event Log after upgrading Kaspersky Security Center Linux from version 16 to version 16.1 if two-factor authentication had been configured for certain users before the upgrade. |
| 16.1 | 9256000 | Fixed an issue where information about managed application components was not available if Network Agent is installed on Microsoft Windows XP. |
| 16.1 | 9251629 | Fixed an issue where some required HTTP response headers were not added when signing in to Kaspersky Security Center Web Console. |

# About Kaspersky Security Center Linux

The section contains information about the purpose of Kaspersky Security Center Linux, its main features and components, and ways to purchase Kaspersky Security Center Linux.

Kaspersky Security Center Linux (also referred to as Kaspersky Security Center) is designed to deploy and manage protection of client devices by using Linux-based Administration Server.

Kaspersky Security Center Linux enables you to install Kaspersky security applications on devices on a corporate network, remotely run scan and update tasks, and manage the security policies of managed applications. As an administrator, you can use a detailed dashboard that provides a snapshot of corporate device statuses, detailed reports, and granular settings in protection policies.

In comparison with Kaspersky Security Center that has Windows®-based Administration Server, Kaspersky Security Center Linux has a different feature set.

Kaspersky Security Center Linux is an application aimed at corporate network administrators and employees responsible for protection of devices in a wide range of organizations.

Using Kaspersky Security Center, you can do the following:

- Create a hierarchy of Administration Servers to manage the organization's network, as well as networks at remote offices or client organizations.

  The *client organization* is an organization whose anti-virus protection is ensured by the service provider.

- Create a hierarchy of administration groups to manage a selection of client devices as a whole.
- Manage an anti-virus protection system built based on Kaspersky applications.
- Perform remote installation of applications by Kaspersky and other software vendors.
- Perform centralized deployment of license keys for Kaspersky applications to client devices, monitor their use, and renew licenses.
- Receive statistics and reports about the operation of applications and devices.
- Receive notifications about critical events during the operation of Kaspersky applications.
- Manage encryption of information stored on hard drives of Windows-based devices and removable drives.
- Manage users' access to encrypted data on Windows-based devices.
- Perform inventory of hardware connected to the organization's network.
- Centrally manage files moved to Quarantine or Backup by security applications, as well as manage files for which processing by security applications has been postponed.

You can purchase Kaspersky Security Center Linux through Kaspersky (for example, at https://www.kaspersky.com ) or through partner companies.

If you purchase Kaspersky Security Center Linux through Kaspersky, you can copy the application from our website. Information that is required for application activation is sent to you by email after payment.

Updates functionality (including providing anti-virus signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

# Distribution kit

At the Kaspersky website, you can download all necessary distribution packages for the application.

The Kaspersky Security Center Linux distribution kit includes the following files:

**Kaspersky Security Center Linux Administration Server:**

- Administration Server to be installed on a device running Debian-based operating system: ksc64_17.0.0-<build>_amd64.deb
- Administration Server to be installed on a device running Red Hat Enterprise Linux-based operating system: ksc64-17.0.0-<build>.x86_64.rpm

**Kaspersky Security Center Web Console:**

- Web Console to be installed on a device running Debian-based operating system: ksc-web-console-17.0.<build>.x86_64.deb
- Web Console to be installed on a device running Red Hat Enterprise Linux-based operating system: ksc-web-console-17.0.<build>.x86_64.rpm

**Kaspersky Security Center installation script:**

- ksc_fast_install.tar.gz

**Network Agent for Windows**:

- Network Agent to be installed on a device with Arm architecture: klnagent_winarm64-17.0.0.<build>-win_<localization>.zip
- Files for the remote installation of Network Agent on a device with x86-32 or x64 architecture: ksc_17_17.0.0.<build>_NetAgent_<localization>.zip
- Files for the remote installation of Network Agent on a device with Arm architecture: ksc_17_17.0.0.<build>_NetAgent_arm64_<localization>.zip
- Files for remote installation via Kaspersky Security Center on a device with Arm architecture: ri_utils_arm64.zip
- Files for remote installation via Kaspersky Security Center on a device with x86-32 or x64 architecture: ri_utils_win32.zip

**Network Agent for Linux:**

- Network Agent to be installed on a device running Debian-based operating system:

  klnagent64_17.0.0-<build>_<architecture>.deb

- Network Agent to be installed on a device running Red Hat Enterprise Linux-based operating system:

  klnagent64-17.0.0-<build>_<architecture>.rpm

- Files for the remote installation of Network Agent on a device running Debian-based operating system:

  klnagent-<architecture>-17.0.0.<build>-deb_<localization>.tar.gz

- Files for the remote installation of Network Agent on a device running Red Hat Enterprise Linux-based operating system:

  klnagent-<architecture>-17.0.0.<build>-rpm_<localization>.tar.gz

- Files for remote installation of Network Agent Elbrus Edition on a device running a Debian-based or Red Hat Enterprise Linux-based operating system:

  klnagent-e2k-17.0.0.<build>-all-<localization>.tar.gz

- Single distribution package for the remote installation of Network Agents for Linux:

  klnagent-all-17.0.0.<build>-all_<localization>.tar.gz

  The single distribution package may be useful if you have many client devices with different CPU architecture and different Linux-based operating systems. The required versions of Network Agents will be automatically selected for further installation on the devices.

- Files for the remote installation of Network Agent on a device running a legacy Debian-based or Red Hat Enterprise Linux-based operating system with glibc 2.5:

  klnagent-all-17.0.0.<build>-glibc2.5-all-<localization>.tar.gz

**Kaspersky Endpoint Detection and Response Optimum web plug-in:**

- signed_irp.zip

  > You can only download the web plug-in from the Repository of distribution packages of applications for remote installation.

If you find it difficult to chose an installation package for a Network Agent for Linux, refer to the article: How to choose the installation package for Network Agent for Linux.

# Hardware and software requirements

- Administration Server requirements
- Web Console requirements
- Network Agent requirements

For Android and iOS version requirements for deploying protection and managing mobile devices, refer to Kaspersky Security for Mobile Help and Kaspersky Secure Mobility Management Help.

# Administration Server requirements

This article lists the software versions on which the application has been tested and for which it is guaranteed to work correctly. The application may also work with other software versions, but those configurations have not undergone a full testing cycle and are not included in the list of guaranteed-supported versions.

Minimum hardware requirements:

- CPU with operating frequency of 2,5 GHz or higher, 2 cores.
- RAM: 6 GB

  You have to turn on the swap file on the device with Administration Server installed. The swap file minimum size must be 1.5 times greater than the RAM volume.
- Available disk space: 10 GB required for the folder where Administration Server data is stored (/var/opt/kaspersky/klnagent_srv).

For more information about the hardware requirements, see the Hardware requirements of the DBMS and Administration Server section.

We recommend that after installing Administration Server on a device, you install Kaspersky Endpoint Security for Linux on this device.
For the concurrent installation, you must have minimum 300 IOPS as well as add to the Administration Server requirements 1,5 GB of RAM, and 15% to the CPU.
For hardware requirements of Kaspersky Endpoint Security, refer to the Kaspersky Endpoint Security for Linux Help.
For information about the security settings required to work with Kaspersky Security Center Linux, refer to the Kaspersky Endpoint Security for Linux Help.

The following operating systems are supported:

For inter-process communication in the operating system, the loopback interface must be available.

- Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm) 64-bit
- Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie) 64-bit
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bit
- Ubuntu Server 24.04 LTS (Noble Numbat) 64-bit
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64-bit
- CentOS Stream 9 64-bit
- CentOS Stream 10 64-bit
- Red Hat Enterprise Linux Server 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64-bit
- Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64-bit

- Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64-bit
- Red Hat Enterprise Linux Server 10.0, 10.1 64-bit
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7 64-bit
- SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7 64-bit
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6) 64-bit
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7) 64-bit
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.8) 64-bit
- Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6) 64-bit
- Astra Linux Special Edition RUSB.10015-17 (operational update 1.7.3) 64-bit
- Astra Linux Special Edition RUSB.10015-03 (operational update 7.6) 64-bit
- Astra Linux Special Edition RUSB.10015-37 (operational update 7.7) 64-bit
- Astra Linux Common Edition (operational update 2.12) 64-bit
- ALT Server 11 64-bit
- ALT SP Server 10 64-bit
- ALT SP Workstation 10 64-bit
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64-bit
- Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9 64-bit
- Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64-bit
- Platform V SberLinux OS Server (SLO) 8.10.1 64-bit
- Platform V SberLinux OS Server (SLO) 9.5.1 64-bit
- Platform V SberLinux OS Server (SLO) 9.6 64-bit
- Platform V SberLinux OS Server (SLO) 9.7 64-bit
- RED OS 7.3 Server 64-bit
- RED OS 7.3 Certified Edition 64-bit
- RED OS 8 64-bit
- ROSA COBALT 7.9 64-bit
- M OS (Moscow Electronic School) 12 Server 64-bit
- Mostech Server 64-bit

- MosOS Server 15.5 64-bit
- MosOS Server 15.6 64-bit

> We recommend that you use the EXT4 file system with its default settings.

The following database servers are supported (can be installed on a different device):

- MySQL Standard Edition 8.0 (release 8.0.20 and later) 32-bit/64-bit
- MySQL Enterprise Edition 8.0 (release 8.0.20 and later) 32-bit/64-bit
- MySQL Standard Edition 8.4 32-bit/64-bit
- MySQL Enterprise Edition 8.4 32-bit/64-bit
- MariaDB 10.11 (build 10.11.10 and later) 32-bit/64-bit
- MariaDB 11.4 64-bit
- MariaDB 11.8 64-bit
- MariaDB 12.3 64-bit
- MariaDB Galera Cluster 4 32-bit/64-bit
- PostgreSQL 15.x 64-bit
- PostgreSQL 15.x 64-bit (cluster Corosync/Pacemaker)
- PostgreSQL 16.x 64-bit (all editions)
- PostgreSQL 17.x 64-bit (all editions)
- PostgreSQL 18.x 64-bit (all editions)
- Postgres Pro 15.x 64-bit (all editions)
- Postgres Pro 15.x 64-bit (cluster Corosync/Pacemaker)
- Postgres Pro 16.x 64-bit (all editions)
- Postgres Pro 16.x Enterprise 64-bit (cluster Built-in High Availability)
- Postgres Pro 17.x 64-bit (all editions)
- Postgres Pro 17.x Enterprise 64-bit (cluster Built-in High Availability)
- Postgres Pro 18.x 64-bit (all editions)
- Postgres Pro 18.x Enterprise 64-bit (cluster Built-in High Availability)
- Platform V Pangolin 6.5.1 64-bit

- Platform V Pangolin 6.5.1 64-bit (cluster Built-in High Availability)
- Platform V Pangolin 7.2.0 64-bit
- Platform V Pangolin 7.2.0 64-bit (Built-in High Availability cluster)
- Jatoba 4 64-bit
- Jatoba 5 64-bit
- Tantor SE 1C 64-bit

When using PostgreSQL or Postgres Pro 18.1–18.5, you may encounter the issue 10671377 described in the article Known limitations and issues.

Highly available PostgreSQL clusters are supported. Refer to the following article for details: Preparing a high availability DBMS cluster for working with Kaspersky Security Center Linux.

For information about the supported virtualization platforms, refer to the Kaspersky Security for Virtualization Light Agent Help.

# Web Console requirements

This article lists the software versions on which the application has been tested and for which it is guaranteed to work correctly. The application may also work with other software versions, but those configurations have not undergone a full testing cycle and are not included in the list of guaranteed-supported versions.

Kaspersky Security Center Web Console Server

Minimum hardware requirements:

- CPU: 2 cores, operating frequency of 2.5 GHz.
- RAM: 4 GB.
- Available disk space: 40 GB required for the folder where Web Console data is stored (/var/opt/kaspersky).

We recommend that after installing Kaspersky Security Center Web Console on a device, you install Kaspersky Endpoint Security for Linux on this device. For Kaspersky Endpoint Security hardware requirements, refer to Kaspersky Endpoint Security for Linux Help.

One of the following operating systems (**64-bit versions only**):

For inter-process communication in the operating system, the loopback interface must be available.

- Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm)
- Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie)

- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- Ubuntu Server 24.04 LTS (Noble Numbat)
- Ubuntu Server 26.04 LTS (Resolute Raccoon)
- CentOS Stream 9
- CentOS Stream 10
- Red Hat Enterprise Linux Server 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10
- Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6
- Red Hat Enterprise Linux Server 10.0, 10.1
- SUSE Linux Enterprise Server 12.5, 12.6, 12.7
- SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6)
- Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6)
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7)
- Astra Linux Special Edition RUSB.10015-17 (operational update 1.7.3)
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.8)
- Astra Linux Special Edition RUSB.10015-03 (update 7.6)
- Astra Linux Special Edition RUSB.10015-37 (operational update 7.7)
- Astra Linux Common Edition (operational update 2.12)
- ALT Server 11
- ALT SP Server 10
- ALT SP Workstation 10
- Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
- Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9
- Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6
- Platform V SberLinux OS Server (SLO) 8.10.1
- Platform V SberLinux OS Server (SLO) 9.5.1
- Platform V SberLinux OS Server (SLO) 9.6

- Platform V SberLinux OS Server (SLO) 9.7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- RED OS 8
- ROSA COBALT 7.9
- M OS (Moscow Electronic School) 12 Server
- Mostech Server
- MosOS Server 15.5
- MosOS Server 15.6

For information about the supported virtualization platforms, refer to the Kaspersky Security for Virtualization Light Agent Help.

### Client devices

For a client device, use of Kaspersky Security Center Web Console requires only a browser.

The minimum screen resolution is 1366x768 pixels.

The hardware and software requirements for the device are identical to the requirements of the browser that is used with Kaspersky Security Center Web Console.

Browsers:

- Google Chrome 154.0.8037.92 or later
- Microsoft Edge 154.0.4258.62 or later
- Safari 18.6 (20621.3.11.11.3) on macOS
- Yandex Browser 26.8.0.1788 or later
- Mozilla Firefox Extended Support Release 140.17.0 or later

## Network Agent requirements

This article lists the software versions on which the application has been tested and for which it is guaranteed to work correctly. The application may also work with other software versions, but those configurations have not undergone a full testing cycle and are not included in the list of guaranteed-supported versions.

Minimum hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit operating system, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Free disk space: 1 GB.

Software requirement for Linux-based devices: the Perl language interpreter version 5.10 or higher must be installed.

**Network Agent. Supported platforms**

| | |
|---|---|
| Operating systems. Microsoft Windows workstations | Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32-bit<br>Microsoft Windows Embedded 7 Standard with Service Pack 1 32-bit/64-bit<br>Microsoft Windows Embedded 8.1 Industry Pro 32-bit/64-bit<br>Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit<br>Microsoft Windows 10 Enterprise 2016 LTSB 32-bit/64-bit<br>Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit<br>Microsoft Windows 10 IoT Enterprise version 1507, 1607, 1703, 1709, 1803, 1809, 1909 32-bit/64-bit<br>Microsoft Windows 10 20H2, 21H2 IoT Enterprise 32-bit/64-bit<br>Microsoft Windows 10 TH1 (July 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 TH2 (November 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 RS1 (August 2016) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 RS2 (April 2017) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 RS4 (April 2018 Update, 17134) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 RS5 (October 2018) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 RS6 (May 2019) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 20H1 (May 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 20H2 (October 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 21H1 (May 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 21H2 (October 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 10 22H2 (October 2023 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit<br>Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM 64-bit<br>Microsoft Windows 11 IoT Enterprise version 25H2 64-bit<br>Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit<br>Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit<br>Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit<br>Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit<br>Microsoft Windows 11 26H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit<br>Microsoft Windows 8.1 Pro/Enterprise 32-bit/64-bit<br>Microsoft Windows 8 Pro/Enterprise 32-bit/64-bit<br>Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium with Service Pack 1 and later 32-bit/64-bit<br>Microsoft Windows XP Professional with Service Pack 2 32-bit/64-bit (supported by Network Agent version 10.5.1781 only)<br>Microsoft Windows XP Professional with Service Pack 3 and later 32-bit (supported by Network Agent version 14.0.0.20023, requires Security Update for Windows XP KB2868626)<br>Microsoft Windows XP Professional for Embedded Systems with Service Pack 3 32-bit (supported by Network Agent version 14.0.0.20023) |

| | |
|---|---|
| Operating systems. Microsoft Windows servers | Microsoft Windows MultiPoint Server 2011 Standard/Premium 64-bit<br>Microsoft Windows Server 2003 SP1 32-bit/64-bit (supported only by Network Agent version 10.5.1781, that you can request through Technical Support)<br>Microsoft Windows Server 2003 SP2 Standard/Enterprise 32-bit/64-bit (supported only by Network Agent version 10.5.1781)<br>Microsoft Windows Server 2003 R2 Standard/Enterprise with SP2 32-bit/64-bit (supported only by Network Agent version 10.5.1781)<br>Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard with Service Pack 1 and later 64-bit<br>Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64-bit<br>Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64-bit<br>Microsoft Windows Server 2016 Datacenter/Standard/Server Core (Installation Option) (LTSB) 64-bit<br>Microsoft Windows Server 2019 Standard/Datacenter/Core 64-bit<br>Microsoft Windows Server 2019 RS5 Essentials/Standard 64-bit<br>Microsoft Windows Server 2022 Standard/Datacenter/Core 64-bit<br>Microsoft Windows Server 2025 Standard/Datacenter/Core 64-bit<br>Microsoft Windows Server 2022 21H2 Standard/Datacenter 64-bit<br>Microsoft Windows Small Business Server 2011 Standard 64-bit<br>Microsoft Windows Small Business Server 2011 Essentials 64-bit |

| | |
|---|---|
| Operating systems. Linux | Debian GNU/Linux 10.0, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12 (Buster) 32-bit/64-bit<br>Debian GNU/Linux 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11 (Bullseye) 32-bit/64-bit<br>Debian GNU/Linux 12.0, 12.1, 12.2, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13 (Bookworm) 32-bit/64-bit<br>Debian GNU/Linux 12.10, 12.11, 12.14 (Bookworm) ARM 64-bit<br>Debian GNU/Linux 13.0, 13.1, 13.2, 13.3 (Trixie) 64-bit<br>Ubuntu Server 10.04 LTS (Lucid Lynx) 32-bit/64-bit<br>Ubuntu Server 16.04 LTS (Xenial Xerus) 32-bit/64-bit<br>Ubuntu Server 18.04 LTS (Bionic Beaver) 64-bit<br>Ubuntu Server 20.04 LTS (Focal Fossa) 64-bit<br>Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bit<br>Ubuntu Server 22.04 LTS ARM 64-bit<br>Ubuntu Server 24.04 LTS (Noble Numbat) 64-bit<br>Ubuntu Server 26.04 LTS (Resolute Raccoon) 64-bit<br>Ubuntu Server 26.04 LTS ARM 64-bit<br>Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32-bit/64-bit<br>Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-bit/64-bit<br>CentOS 5.2 64-bit (supported only by Network Agent for Linux Legacy, which you can download by using the Web Console interface or from the Kaspersky website)<br>CentOS 5.4 64-bit (supported only by Network Agent for Linux Legacy, which you can download by using the Web Console interface or from the Kaspersky website)<br>CentOS 6.4 64-bit (supported only by Network Agent for Linux Legacy, which you can download by using the Web Console interface or from the Kaspersky website)<br>CentOS 6.6 32-bit/64-bit (supported only by Network Agent for Linux Legacy, which you can download by using the Web Console interface or from the Kaspersky website)<br>CentOS 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64-bit<br>CentOS Stream 8 64-bit<br>CentOS Stream 9 64-bit<br>CentOS Stream 9 ARM 64-bit<br>CentOS Stream 10 64-bit<br>Red Hat Enterprise Linux Server 6.5, 6.6, 6.7, 6.8, 6.9, 6.10 32-bit/64-bit<br>Red Hat Enterprise Linux Server 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64-bit<br>Red Hat Enterprise Linux Server 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64-bit<br>Red Hat Enterprise Linux Server 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64-bit<br>Red Hat Enterprise Linux Server 10.0, 10.1 64-bit<br>SUSE Linux Enterprise Server 12.5, 12.6, 12.7 64-bit<br>SUSE Linux Enterprise Server 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7 64-bit<br>SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7 ARM 64-bit<br>openSUSE Leap 15.0, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6 64-bit<br>EulerOS 2.0 SP10 64-bit<br>EulerOS 2.0 SP10 ARM 64-bit<br>Astra Linux Special Edition RUSB.10015-01 (operational update 1.4) 32-bit<br>Astra Linux Special Edition RUSB.10015-01 (operational update 1.4) 64-bit (supported only by Network Agent for Linux Legacy, which you can download by using the Web Console interface or from the Kaspersky website)<br>Astra Linux Special Edition RUSB.10015-01 (operational update 1.5) 64-bit<br>Astra Linux Special Edition RUSB.10015-01 (operational update 1.6) 64-bit<br>Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6) 64-bit<br>Astra Linux Special Edition RUSB.10015-16 (release 2) (operational update 8.1) E2K<br>Astra Linux Special Edition RUSB.10015-17 (operational update 1.7.3) 64-bit<br>Astra Linux Special Edition RUSB.10015-01 (operational update 1.7) 64-bit<br>Astra Linux Special Edition RUSB.10015-01 (operational update 1.8) 64-bit<br>Astra Linux Special Edition RUSB.10015-03 (operational update 7.6) 64-bit<br>Astra Linux Special Edition RUSB.10015-37 (operational update 7.7) 64-bit<br>Astra Linux Special Edition RUSB.10152-02 (operational update 4.7) ARM 64-bit<br>Astra Linux Special Edition RUSB.10265-01 (operational update 8.1) E2K<br>Astra Linux Common Edition (operational update 2.12) 64-bit<br>ALT Workstation 11.2 ARM 64-bit<br>ALT Workstation 11 64-bit |

ALT Server 11.1 ARM 64-bit
ALT Server 11 64-bit
ALT Education 11 64-bit
ALT Workstation 10.1 64-bit
ALT Server 10.1 64-bit
ALT Education 10.1 64-bit
ALT SP Server 10 32-bit/64-bit
ALT SP Server 10 ARM 64-bit
ALT SP Server 10 E2K
ALT SP Workstation 10 32-bit/64-bit
ALT SP Workstation 10 ARM 64-bit
ALT SP Workstation 10 E2K
ALT 8 SP Server (LKNV.11100-01) 32-bit/64-bit
ALT 8 SP Server (LKNV.11100-02) 32-bit/64-bit
ALT 8 SP Server (LKNV.11100-03) 32-bit/64-bit
ALT SP Server 8 E2K
ALT 8 SP Workstation (LKNV.11100-01) 32-bit/64-bit
ALT 8 SP Workstation (LKNV.11100-02) 32-bit/64-bit
ALT 8 SP Workstation (LKNV.11100-03) 32-bit/64-bit
ALT 8 SP Workstation E2K
Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 64-bit
Oracle Linux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64-bit
Oracle Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7 64-bit
Linux Mint 21.1, 21.2, 21.3 64-bit
Linux Mint 22.0, 22.1, 22.2 64-bit
AlterOS 7.5 64-bit
AlterOS 2025 64-bit
SberOS 3.4.0 64-bit
SberOS 3.5.0 64-bit
SberOS 3.6.1 64-bit
Platform V SberLinux OS Server (SLO) 8.10.1 64-bit
Platform V SberLinux OS Server (SLO) 9.1 64-bit
Platform V SberLinux OS Server (SLO) 9.5.1 64-bit
Platform V SberLinux OS Server (SLO) 9.6 64-bit
Platform V SberLinux OS Server (SLO) 9.7 64-bit
RED OS 7.3 Server 64-bit
RED OS 7.3 Certified Edition 64-bit
RED OS 8 64-bit
RED OS 8 ARM 64-bit
ROSA Enterprise Linux Server 7.9 64-bit
ROSA Enterprise Linux Desktop 7.9 64-bit
ROSA COBALT 7.9 64-bit
ROSA CHROME 12 64-bit
AlmaLinux 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64-bit
AlmaLinux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64-bit
Rocky Linux 8.5, 8.6, 8.7, 8.8, 8.9, 8.10 64-bit
Rocky Linux 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 64-bit
Atlant, Alcyone build, version 2022.02 64-bit
MSVSPHERE 9.2 SERVER 64-bit
MSVSPHERE 9.2 ARM 64-bit
MSVSPHERE 9.4 SERVER 64-bit
MSVSPHERE 9.4 ARM 64-bit
MSVSPHERE 9.5 SERVER 64-bit
MSVSPHERE 9.5 ARM 64-bit
SynthesisM Server 8.6 64-bit
SynthesisM Client 8.6 64-bit

| | |
|---|---|
| | OSnova 2.9, 2.14 64-bit<br>OSnova 3.0.5, 3.1 64-bit<br>Kylin 10 64-bit<br>EMIAS 1.0 64-bit<br>Amazon Linux 2 64-bit<br>Amazon Linux 2023 64-bit<br>MosOS Server 15.5 64-bit<br>MosOS Server 15.6 64-bit<br>OS MES 12 for Moscow schools for desktops and laptops (with telemetry and DIT support) 64-bit.<br>OS MES 12 for Moscow schools for interactive panels (with telemetry and DIT support) 64-bit.<br>M OS (Moscow Electronic School) 12 Server 64-bit<br>Mostech 64-bit<br>Mostech Server 64-bit<br>Fedora Linux Server 41 64-bit<br>Fedora Linux Workstation 41 64-bit<br>Elbrus 9.3.6 E2K |
| Operating systems. macOS | For the list of supported operating systems, refer to the Kaspersky Endpoint Security for Mac Help. |
| Virtualization platforms | For information about the supported virtualization platforms, refer to the Kaspersky Security for Virtualization Light Agent Online Help. |

On Windows versions older than Microsoft Windows Server 2008 R2 (server versions) and Microsoft Windows 7 (desktop versions) Network Agent does not support the following functionality:

- Updates retranslation (used by distribution points)
- KSN proxy (used by distribution points)
- Vulnerability scan task

On the devices running Microsoft Windows 10 version RS4 or RS5, Kaspersky Security Center might be unable to detect some vulnerabilities in folders where case sensitivity is enabled.

Before installing Network Agent on the devices running Windows 7, Windows Server 2008 R2 or Windows MultiPoint Server 2011, make sure that you have installed the security update KB3063858 for OS Windows (Security Update for Windows 7 (KB3063858), Security Update for Windows 7 for x64-based Systems (KB3063858), Security Update for Windows Server 2008 R2 x64 Edition (KB3063858).

In Microsoft Windows XP, Network Agent might not perform some operations correctly.

You can install or update Network Agent for Windows XP in Microsoft Windows XP only. The supported editions of Microsoft Windows XP and their corresponding versions of the Network Agent are listed in the list of supported operating systems. You can download the required version of the Network Agent for Microsoft Windows XP from this page.

We recommend that you install the same version of the Network Agent for Linux as Kaspersky Security Center Linux.

Kaspersky Security Center Linux fully supports Network Agent of the same or newer versions.

Network Agent for macOS is provided together with Kaspersky security application for this operating system.

# Compatible Kaspersky applications and solutions

Kaspersky Security Center Linux supports centralized deployment and management of all Kaspersky applications and solutions that are currently supported. To find out versions of the applications and solutions, refer to the Application Support Lifecycle webpage.

Supported Kaspersky applications:

- Kaspersky Endpoint Security for Windows (supports file servers)
- Kaspersky Endpoint Security for Linux (supports file servers)
- Kaspersky Endpoint Security for Linux Elbrus Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security for Android
- Kaspersky Endpoint Security for Aurora
- Kaspersky Security for iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux
- Kaspersky Security for Virtualization Light Agent
- KATA Sandbox (one of the Kaspersky Anti Targeted Attack Platform components)
- Kaspersky Thin Client
- Kaspersky NGFW
- Kaspersky Sandbox

- Kaspersky Password Manager for Business
- Kaspersky Vulnerability Management

Kaspersky Security Center Linux is included in the following solutions:

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response
- Kaspersky Next XDR Optimum

To find out versions of the applications and solutions, refer to the Application Support Lifecycle webpage.

### Known issues and limitations

Single Sign-On (SSO) is not supported for Kaspersky Industrial CyberSecurity for Networks.

# About compatibility of Kaspersky Security Center Linux components

In the table below, you can find information about the compatibility of Kaspersky Security Center Linux components.

Compatibility of Kaspersky Security Center Linux components

| Component | Compatible with |
|---|---|
| Kaspersky Security Center 17 Linux Administration Server | • Kaspersky Security Center Web Console of the following versions: 17, 16.3, 16.2<br>• Kaspersky Security Center Network Agent of the following versions: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 14*, 10.5** |
| Kaspersky Security Center 17 Web Console | Kaspersky Security Center Linux Administration Server of the following versions: 17, 16.3, 16.2 |
| Kaspersky Security Center 17 Linux primary Administration Server | Secondary Administration Servers:<br>• Kaspersky Security Center Linux of the following versions: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1<br>• Kaspersky Security Center Windows of the following versions: 15.1 |
| Kaspersky Security Center 17 Linux secondary Administration Server | Primary Administration Servers:<br>• Kaspersky Security Center Linux of the following versions: 17, 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1<br>• Kaspersky Security Center Windows of the following versions: 15.1 |
| Kaspersky Security Center 17 Network Agent | Administration Servers:<br>• Kaspersky Security Center Linux of the following versions: 17, 16.3, 16.2, 16.1, 16.0, 15.4, 15.3, 15.2, 15.1<br>• Kaspersky Security Center Windows of the following versions: 15.1 |
| Backup and restore of Kaspersky Security Center Administration Server data | Data backup and restore is supported from the following Kaspersky Security Center Linux Administration Server versions:<br>16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1 |

*This version supports Microsoft Windows XP Professional with Service Pack 3. You can download this Network Agent version from this page.

**This version supports Microsoft Windows XP Professional with Service Pack 2. You can request this Network Agent version through Technical Support.

We recommend that you use the latest version of both Kaspersky Security Center Administration Server and Kaspersky Security Center Web Console. Otherwise, the functionality of Kaspersky Security Center may be limited. You can install and upgrade Kaspersky Security Center Administration Server and Kaspersky Security Center Web Console independently. In this case you should ensure that the version of the installed Kaspersky Security Center Web Console is compatible with the version of the Administration Server to which you connect:

If you have the latest version of Kaspersky Security Center Web Console and the previous version of Kaspersky Security Center, and an error occurs during domain authentication, the error text will contain a default message.

# Comparison of Kaspersky Security Center: Windows-based vs. Linux-based

Kaspersky provides Kaspersky Security Center as an on-premises solution for two platforms—Windows and Linux. In the solution for Windows, you install the Administration Server on a device running a Windows operating system. The solution for Linux has a version of the Administration Server that can be installed on a Linux device. This Online Help contains information about Kaspersky Security Center. For detailed information about the Windows-based solution, refer to the Kaspersky Security Center Windows Help.

The table below lets you compare the main features of Kaspersky Security Center as a Windows-based solution and as a Linux-based solution.

Feature comparison of Kaspersky Security Center working as a Windows-based solution and Linux-based solution

| Feature or property | Kaspersky Security Center 15.1 Windows | Kaspersky Security Center 16.3 Linux |
|---|---|---|
| **Administration Server** | | |
| Database management system (DBMS) location | On-premises | On-premises<br>(Microsoft SQL is not supported) |
| Operating system to install Administration Server on | Windows | Linux |
| Hierarchy of Administration Servers | ✓ | ✓ |
| Support for virtual Administration Servers | ✓ | ✓ |
| Deployment of the Kaspersky Security Center failover cluster | ✓<br>A single-site cluster only | ✓<br>Starting from Kaspersky Security Center 16.2 Linux, geo-distributed failover cluster is supported |
| Using SNMP to send Administration Server statistics to third-party applications | ✓ | ✓ |
| Web Server for publishing installation packages and other files | ✓ | ✓ |
| **Administration Console** | | |
| Administration console type | MMC-based and web-based | Web-based |
| Operating system to install the web-based administration console on | Windows or Linux | Linux |

| Feature or property | Kaspersky Security Center 15.1 Windows | Kaspersky Security Center 16.3 Linux |
|---|---|---|
| Sign-in to the console by using domain authentication | ✓ | ✓ |
| **Managing client devices and administration groups** | | |
| Maximum number of managed devices (per one Administration Server) | 100,000 (with Microsoft SQL Server) | 50,000 (with PostgreSQL and Postgres Pro) |
| Network polling | ✓ | ✓ |
| Protection of Windows, macOS, and Linux-managed devices | ✓ | ✓ |
| Protection of mobile devices | ✓<br>Basic management of mobile devices | ✓<br>MDM and using the Kaspersky Secure Mobility Management functionality (under the license) |
| Protection management of virtual machines | ✓ | ✓ |
| Protection of public cloud infrastructure | ✓ | — |
| Remotely connecting to the desktop of a client device | ✓ | ✓ |
| Data encryption and protection | ✓<br>On Windows-based managed devices with Kaspersky Endpoint Security for Windows or Kaspersky Endpoint Security for Mac installed | ✓<br>On Windows-based managed devices with Kaspersky Endpoint Security for Windows or Kaspersky Endpoint Security for Mac installed |
| Support of clusters and server arrays in administration groups | ✓ | ✓ |
| Administration group hierarchy | ✓ | ✓ |
| Adding a connection gateway in the DMZ as a distribution point | ✓<br>(not supported for Web Console) | ✓ |
| **Working with users** | | |
| Creating and managing user accounts | ✓ | ✓ |
| **Managing Kaspersky applications** | | |
| Application policies | ✓ | ✓ |
| Tasks for Kaspersky applications | ✓ | ✓ |
| Kaspersky Security Network | ✓ | ✓ |
| KSN proxy server | ✓ | ✓ |
| Kaspersky Private Security Network | ✓ | ✓ |
| Centralized deployment of license keys for Kaspersky applications | ✓ | ✓ |
| Remote diagnostics of client devices | ✓ | ✓ |
| Updating Kaspersky applications automatically | ✓ | ✓ |
| Support for Adaptive Anomaly Control | ✓ | ✓ |
| Device-centric security management | ✓ | ✓ |
| User-centric security management | ✓ | ✓ |
| **Systems management** | | |
| Deploying operating systems on client devices | ✓ | — |
| Managing third-party licenses | ✓ | To be implemented in 2026 |
| Using Administration Server as WSUS server | ✓ | ✓<br>(passive Windows Update search mode only) |

| Feature or property | Kaspersky Security Center 15.1 Windows | Kaspersky Security Center 16.3 Linux |
|---|---|---|
| **Managing third-party applications on client devices** | | |
| Installing third-party software updates and fixing third-party software vulnerabilities | ✓ | ✓ |
| Importing and exporting application categories | ✓ (not supported for Web Console) | To be implemented in 2026 |
| **Monitoring, reporting, and audit** | | |
| Managing object revisions | ✓ | ✓ |
| Comparing policy revisions | ✓ | ✓ |
| Viewing and working with alerts detected by Kaspersky Endpoint Detection and Response Optimum | ✓ | ✓ |
| Notifications about events that occurred on managed devices | ✓ | ✓ |
| Monitoring the policies status and tasks status | ✓ | ✓ |
| **Integrations** | | |
| Kaspersky Managed Detection and Response integration | ✓ | ✓ |
| Integration with SIEM systems | ✓ | ✓ |
| Aggregating alerts and performing response actions using Active Directory, KASAP, and Kaspersky TIP Sandbox | – | ✓ You must activate Administration Server under a Kaspersky Next XDR Optimum license, and then deploy the Kaspersky Next XDR Optimum license key to your managed applications |

# About Kaspersky Next Expert View

Using Kaspersky Security Center as an on-premises application means that you install Kaspersky Security Center, including Administration Server, on a local device and manage the network security system through the Microsoft Management Console-based Administration Console (available only in Kaspersky Security Center Windows) or Kaspersky Security Center Web Console.

However, you can use Kaspersky Security Center as a cloud service instead. In this case Kaspersky Security Center is installed and maintained for you by Kaspersky experts in the cloud environment, and Kaspersky gives you access to the Administration Server as a service. You manage the network security system through the cloud-based Administration Console named Kaspersky Next Expert View. This console has an interface similar to the interface of Kaspersky Security Center Web Console.

The interface and documentation of Kaspersky Next Expert View are available in the following languages:

- English
- French
- German
- Italian
- Japanese

- Portuguese (Brazil)
- Russian
- Simplified Chinese
- Spanish
- Spanish (LATAM)
- Traditional Chinese

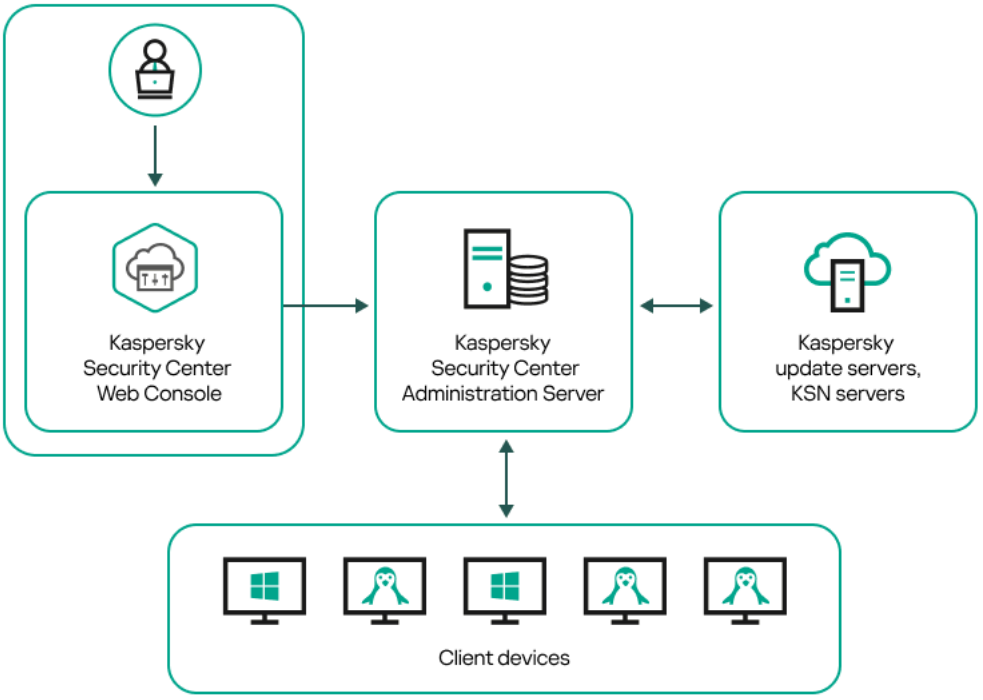
More information about Kaspersky Next Expert View and its features is available in the Kaspersky Next Expert View documentation and in the Kaspersky Endpoint Security for Business documentation.

# Architecture and basic concepts

This section explains the application architecture and basic concepts related to Kaspersky Security Center Linux.

## Architecture

This section provides a description of the components of Kaspersky Security Center and their interaction.



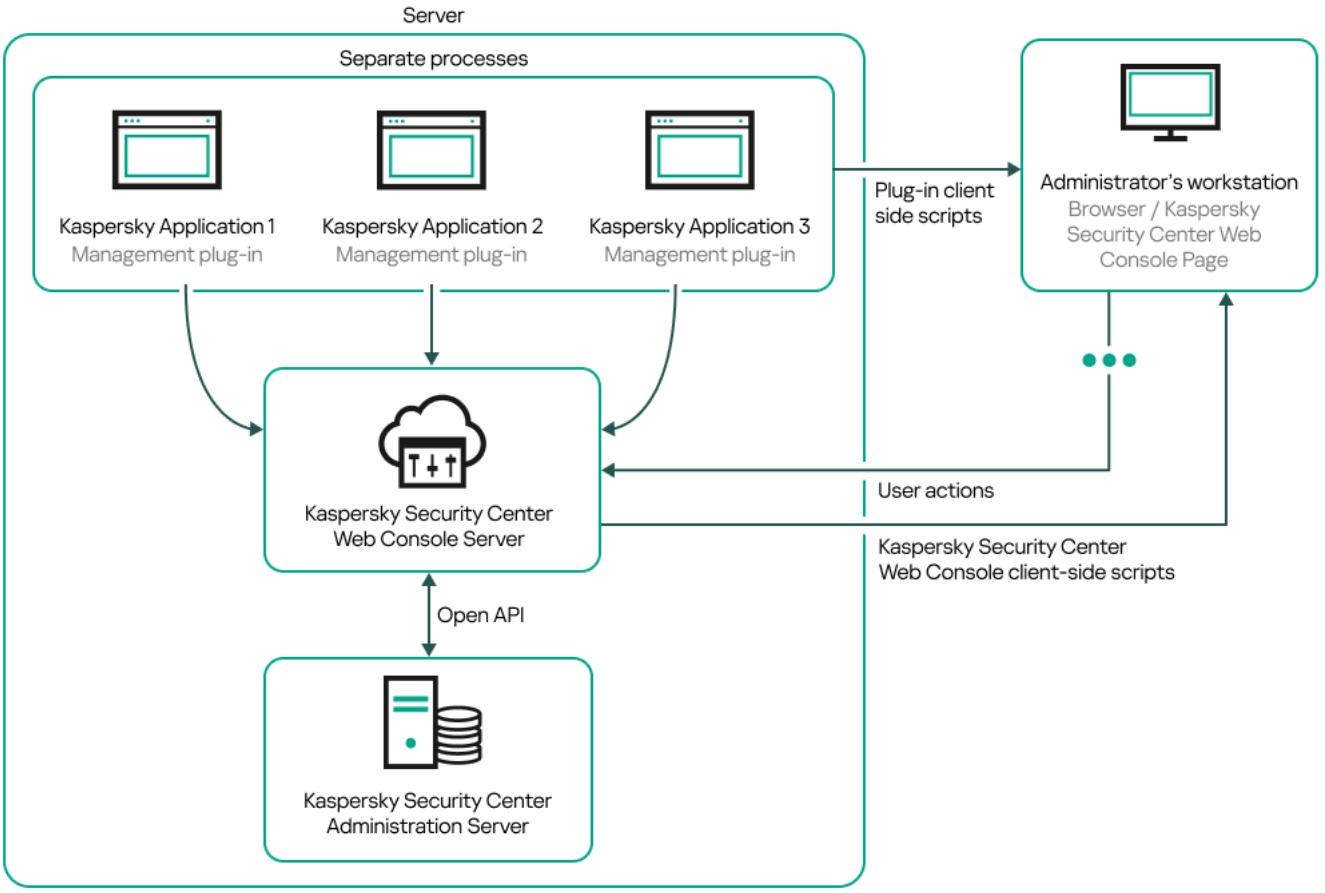

Kaspersky Security Center Linux architecture

Kaspersky Security Center Linux comprises the following main components:

- **Kaspersky Security Center Web Console**. Provides a web interface for creating and maintaining the protection system of a client organization's network that is managed by Kaspersky Security Center.
- **Kaspersky Security Center Administration Server** (also referred to as *Server*). Centralizes storage of information about applications installed on the organization's network and about how to manage them.
- **Kaspersky update servers**. HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates.
- **KSN servers**. Servers that contain a Kaspersky database with constantly updated information about the reputation of files, web resources, and software. Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false positives.
- **Client devices.** A client company's devices protected by Kaspersky Security Center Linux. Each device that has to be protected must have one of the Kaspersky security applications installed.

# Deployment diagram of Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console

The figure below shows the deployment diagram of Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console.




Deployment diagram of Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console

Management plug-ins for Kaspersky applications installed on protected devices (one plug-in for each application) are deployed together with Kaspersky Security Center Web Console Server.

As an administrator, you access Kaspersky Security Center Web Console by using a browser on your workstation.

When you perform specific actions in Kaspersky Security Center Web Console, Kaspersky Security Center Web Console Server communicates with Kaspersky Security Center Linux Administration Server through OpenAPI. Kaspersky Security Center Web Console Server requests the required information from Kaspersky Security Center Linux Administration Server and displays the results of your operations in Kaspersky Security Center Web Console.

# Ports used by Kaspersky Security Center Linux

The tables below show the default ports used by Administration Server and by client devices. If you want, you can change each of these default port numbers.

Ports used by Kaspersky Security Center Linux Administration Server

| Port number | Name of the process that opens the port | Protocol | Port purpose | Scope |
|---|---|---|---|---|
| 8060 | klcsweb | TCP | Transmitting published installation packages to client devices | Publishing installation packages.<br>You can change the default port number in the **Web Server** section of the Administration Server properties window.<br>This port is optional. For security reasons we recommend using 8061 TCP port. |
| 8061 | klcsweb | TCP (TLS) | Transmitting published installation packages to client devices | Publishing installation packages.<br>You can change the default port number in the **Web Server** section of the Administration Server properties window. |
| 13000 | klserver | TCP (TLS) | Receiving connections from Network Agents and secondary Administration Servers; also used on secondary Administration Servers for receiving connections from the primary Administration Server (for example, if the secondary Administration Server is in DMZ) | Managing client devices and secondary Administration Servers.<br>You can change the default port number for incoming connections from Network Agents when configuring connection ports during installation of Kaspersky Security Center Linux. You can change the default port for incoming connections from secondary Administration Servers when creating the hierarchy of Administration Servers. |
| 13000 | klserver | UDP | Receiving information about devices that were turned off from Network Agents | Managing client devices.<br>You can change the default port number in the Network Agent policy settings. |
| 13291 | klserver | TCP (TLS) | Using the klakaut utility to automate the Kaspersky Security Center Linux operation | Working with the klakaut utility. The klakaut utility and a Help system for it are located in the Kaspersky Security Center Linux installation folder.<br>This port is closed by default. If you want to use the klakaut utility to automate the Kaspersky Security Center Linux operation, open the 13291 port by using the klscflag utility. |
| 13299 | klserver | TCP (TLS) | Receiving connections from Identity and Access Manager (IAM) to Administration Server; receiving connections to Administration Server over OpenAPI | Managing Administration Server by using Kaspersky Security Center Web Console; working with OpenAPI.<br>You can change the default port number in the Administration Server properties window (in the **Connection ports** subsection of the **General** section), or when creating a hierarchy of Administration Servers. |
| 14000 | klserver | TCP | Receiving connections from Network Agents | Managing client devices.<br>You can change the default port number when configuring connection ports during the installation of Kaspersky Security Center Linux, or when manually connecting a client device to the Administration Server.<br>This port is optional and is closed by default. For security reasons we recommend using 13000 TCP port. |

| Port number | Name of the process that opens the port | Protocol | Port purpose | Scope |
|---|---|---|---|---|
| 13111 (only if KSN proxy service is run on the device) | ksnproxy | TCP | Receiving requests from managed devices to KSN proxy server | KSN proxy server.<br>You can change the default port number in the Administration Server properties window. |
| 15111 (only if KSN proxy service is run on the device) | ksnproxy | UDP | Receiving requests from managed devices to KSN proxy server | KSN proxy server.<br>You can change the default port number in the Administration Server properties window. |
| 17111 (only if KSN proxy service is run on the device) | ksnproxy | HTTPS | Receiving requests from managed devices to KSN proxy server | KSN proxy server.<br>You can change the default port number in the Administration Server properties window. |
| 17000 | klactprx | TCP (TLS) | Receiving connections for application activation from managed devices | Activation proxy server for managed devices.<br>You can change the default port number in the Administration Server properties window (in the **Additional ports** subsection of the **General** section). |
| 13292 (only if you manage mobile devices) | klserver | TCP (TLS) | Receiving connections from mobile devices | Mobile Device Management.<br>You can change the default port number in the Administration Server properties window in the Administration Console or in Kaspersky Security Center Web Console. |
| 19170 | klserver | HTTPS (TLS) | Tunneling connections to managed devices by using the klsctunnel utility | Remotely connecting to managed devices by using Kaspersky Security Center Web Console.<br>You can change the default port number in the Administration Server properties window (**General** → **Connection ports** → **RDP connection tunneling**). |
| 4444 | kliam | HTTPS | Authentication by using the OpenID Connect protocol | Exchange of authentication tokens between the browser and Identity and Access Manager (IAM). |
| 9050 | kliam | HTTPS | Connection to the Administration Server by using IAM | Exchange of authentication tokens between Kaspersky Security Center Web Console and IAM. |

If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MariaDB). Please refer to the DBMS documentation for the relevant information.

The table below shows the port used by the iOS™ MDM Server (only if you manage mobile devices).

Port used by iOS MDM Server

| Port number | Name of the process that opens the port | Protocol | Port purpose | Scope |
|---|---|---|---|---|
| 443 | kliosmdmservicesrv | TCP (TLS) | Receiving connections from iOS mobile devices | Mobile Device Management.<br>You can change the default port number when installing iOS MDM Server. |

The table below shows the port used by Kaspersky Security Center Web Console Server. It can be the same device where Administration Server is installed or a different device.

Port used by Kaspersky Security Center Web Console Server

| Port number | Name of the process that opens the port | Protocol | Port purpose | Scope |
|---|---|---|---|---|
| 8080 | Node.js: Server-side JavaScript | TCP (TLS) | Receiving connections from browser to Kaspersky Security Center Web Console | Kaspersky Security Center Web Console.<br>You can change the default port number when installing Kaspersky Security Center Web Console. If you install Kaspersky Security Center Web Console on the ALT Linux operating system, you must specify a port number other than 8080, because port 8080 is used by the operating system. |

The table below shows the ports used by managed devices where Network Agent is installed.

Ports used by Network Agent

| Port number | Name of the process that opens the port | Protocol | Port purpose | Scope |
|---|---|---|---|---|
| 15000 | klnagent | UDP | Management signals from Administration Server or distribution point to Network Agents | Managing client devices.<br>You can change the default port number in the Network Agent policy settings. |
| 15000 | klnagent | UDP broadcast | Getting data about other Network Agents within the same broadcasting domain (the data is then sent to the Administration Server) | Delivering updates and installation packages. |
| 15001 | klnagent | UDP | Receiving multicast requests from a distribution point (if in use) | Receiving updates and installation packages from a distribution point.<br>You can change the default port number in the distribution point properties window. |
| 30522,<br>30523 (ports on the localhost interface) | klnagent | TCP | Transferring application updates from Network Agent to locally installed Kaspersky applications by using the FileTransferBridge component | Managed devices that receive Kaspersky application updates from Administration Server specified as a database update source. |

Please note that the klnagent process can also request free ports from the dynamic port range of an endpoint operating system. These ports are allocated to the klnagent process automatically by the operating system, so klnagent process can use some ports that are used by another software. If the klnagent process affects that software operations, change the port settings in this software, or change the default dynamic port range in your operating system to exclude the port used by the software affected.

Also take into account that recommendations on the compatibility of Kaspersky Security Center Linux with third-party software are described for reference only and may not be applicable to new versions of third-party software. The described recommendations for configuring ports are based on the experiences of Technical Support and our best practices.

The table below shows the ports used by a managed device with Network Agent installed acting as a distribution point. The listed ports are used by the distribution point devices in addition to the ports used by Network Agents (see table above).

Ports used by Network Agent functioning as distribution point

| Port number | Name of the process that opens the port | Protocol | Port purpose | Scope |
|---|---|---|---|---|
| 13000 | klnagent | TCP (TLS) | Receiving connections from Network Agents and connection gateways | Managing client devices, delivering updates and installation packages.<br>You can change the default port number in the distribution point properties. |
| 13111 (only if KSN proxy service is run on the device) | ksnproxy | TCP | Receiving requests from managed devices to KSN proxy server | KSN proxy server.<br>You can change the default port number in the distribution point properties. |

| Port number | Name of the process that opens the port | Protocol | Port purpose | Scope |
|---|---|---|---|---|
| 15111 (only if KSN proxy service is run on the device) | ksnproxy | UDP | Receiving requests from managed devices to KSN proxy server | KSN proxy server.<br>You can change the default port number in the distribution point properties. |
| 17111 (only if KSN proxy service is run on the device) | ksnproxy | HTTPS | Receiving requests from managed devices to KSN proxy server | KSN proxy server.<br>You can change the default port number in the distribution point properties. |
| 13295 (only if you use the distribution point as a push server) | klnagent | TCP (TLS) | Receiving connections from client devices | Push server.<br>You can change the default port number in the distribution point properties. |
| 8060 | klcsweb | TCP | Transmitting published installation packages to client devices | Publishing installation packages.<br>You can change the default port number in the **Web Server** section of the Administration Server properties window. |
| 8061 | klcsweb | TCP (TLS) | Transmitting published installation packages to client devices | Publishing installation packages.<br>You can change the default port number in the **Web Server** section of the Administration Server properties window. |

The table below shows ports used on a domain controller device.

Ports used on a domain controller device

| Port number | Protocol | Port purpose | Scope |
|---|---|---|---|
| 389 | LDAP over TCP or UDP | Connecting to a LDAP server | Domain controller polling |
| 636 | LDAP over TLS | Connecting to a LDAP server | Domain controller polling |

The table below contains the port that must be open on client devices where Network Agent is not installed.

Port used on the unassigned client device

| Port number | Protocol | Port purpose | Scope |
|---|---|---|---|
| 22 | SSH | Connecting to a client device over SSH | Remote installation of Kaspersky applications. |

# Ports used by Kaspersky Security Center Web Console

The table below lists the ports that must be open on the device where Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) is installed.

Ports used by Kaspersky Security Center Web Console

| Port number | Service name | Protocol | Port purpose | Scope |
|---|---|---|---|---|
| 2001 | Kaspersky Security Center Product Plugins Server | HTTPS | API port that is used by the management plug-in processes to receive requests from the "Kaspersky Security Center Web Console Management Service". | Running node processes of management plug-ins |
| 1329, 2003 | Kaspersky Security Center Web Console Management Service | HTTPS | API ports that are used to receive requests from the "Kaspersky Security Center Web Console Management Service" running on the same device. | Updating Kaspersky Security Center Web Console components |
| 2005 | Kaspersky Security Center Web Console | HTTPS | API port that is used to receive requests from the "Kaspersky Security Center Web Console Management Service" running on the same device. | Running node processes of Kaspersky Security Center Web Console |

| Port number | Service name | Protocol | Port purpose | Scope |
|---|---|---|---|---|
| 4222 | Kaspersky Security Center Web Console NATS | HTTPS | API ports of the NATS-based Message Broker that are used for communication between processes of both Kaspersky Security Center Web Console and management plug-ins.<br>The 8222 port is used to monitor NATS. | Interaction between Kaspersky Security Center Web Console and management plug-ins |
| 4444 | Identity and Access Manager (IAM) | HTTPS | Port that is used by the OpenID Connect authentication protocol. | Exchange of authentication tokens between Kaspersky Security Center Web Console and Identity and Access Manager (IAM) |
| 9050 | IAM | HTTPS | Port that is used by IAM. | Interaction between Kaspersky Security Center Web Console and IAM |

# Basic concepts

This section explains basic concepts related to Kaspersky Security Center Linux.

## Administration Server

Kaspersky Security Center Linux components enable remote management of Kaspersky applications installed on client devices.

Devices with the Administration Server component installed will be referred to as *Administration Servers* (also referred to as *Servers*). Administration Servers must be protected, including physical protection, against any unauthorized access.

Administration Server is installed on a device as a service with the following set of attributes:

- With the name `kladminserver_srv`
- Set to start automatically when the operating system starts
- With the `ksc` account or the user account selected during the installation of Administration Server

Refer to the following article for the full list of installation settings: Installing Kaspersky Security Center Linux.

Administration Server performs the following functions:

- Storage of the administration groups' structure
- Storage of information about the configuration of client devices
- Organization of repositories for application distribution packages
- Remote installation of applications to client devices and removal of applications
- Updating application databases and software modules of Kaspersky applications
- Management of policies and tasks on client devices

- Storage of information about events that have occurred on client devices
- Generation of reports on the operation of Kaspersky applications
- Deployment of license keys to client devices and storing information about the license keys
- Forwarding notifications about the progress of tasks (such as detection of viruses on a client device)

Naming Administration Servers in the application interface

In the interface of the Kaspersky Security Center Web Console, Administration Servers can have the following names:

- Name of the Administration Server device, for example: "*device_name*" or "Administration Server: *device_name*".
- IP address of the Administration Server device, for example: "*IP_address*" or "Administration Server: *IP_address*".
- Secondary Administration Servers and virtual Administration Servers have custom names that you specify when you connect a virtual or a secondary Administration Server to the primary Administration Server.
- If you use Kaspersky Security Center Web Console installed on a Linux device, the application displays the names of the Administration Servers that you specified as trusted in the response file.

You can connect to Administration Server by using Kaspersky Security Center Web Console.

# Hierarchy of Administration Servers

Administration Servers can be arranged in a hierarchy. Each Administration Server can have several secondary Administration Servers (referred to as *secondary Servers*) on different nesting levels of the hierarchy. The nesting level for secondary Servers is unrestricted. The administration groups of the primary Administration Server will then include the client devices of all secondary Administration Servers. Thus, isolated and independent sections of networks can be managed by different Administration Servers which are in turn managed by the primary Server.

In a hierarchy, a Linux-based Administration Server can work both as a primary Server and as a secondary Server. The primary Linux-based Server can manage both Linux-based and Windows-based secondary Servers. A primary Windows-based Server can manage a secondary Linux-based Server.

*Virtual Administration Servers* are a particular case of secondary Administration Servers.

The hierarchy of Administration Servers can be used to do the following:

- Decrease the load on Administration Server (compared to a single installed Administration Server for an entire network).
- Decrease intranet traffic and simplify work with remote offices. You do not have to establish connections between the primary Administration Server and all networked devices, which may be located, for example, in different regions. It is sufficient to install a secondary Administration Server in each network segment, distribute devices among administration groups of secondary Servers, and establish connections between the secondary Servers and the primary Server over fast communication channels.

- Distribute responsibilities among the anti-virus security administrators. All capabilities for centralized management and monitoring of the anti-virus security status in corporate networks remain available.
- Use Kaspersky Security Center Linux by service providers. The service provider only needs to install Kaspersky Security Center Linux and Kaspersky Security Center Web Console. To manage a large number of client devices of various organizations, a service provider can add secondary Administration Servers (including virtual Servers) to the hierarchy of Administration Servers.

Each device included in the hierarchy of administration groups can be connected to one Administration Server only. You must independently monitor the connection of devices to Administration Servers. Use the feature for device search in administration groups of different Servers based on network attributes.

# Virtual Administration Server

Virtual Administration Server (also referred to as *virtual Server*) is a component of Kaspersky Security Center Linux intended for managing anti-virus protection of the network of a client organization.

Virtual Administration Server is a particular case of a secondary Administration Server and has the following restrictions as compared with a physical Administration Server:

- Virtual Administration Server can be created only on a primary Administration Server.
- Virtual Administration Server uses the primary Administration Server database in its operation. Data backup and restoration tasks, as well as update scan and download tasks, are not supported on a virtual Administration Server.
- Virtual Server does not support creation of secondary Administration Servers (including virtual Servers).

In addition, virtual Administration Server has the following restrictions:

- In the virtual Administration Server properties window, the number of sections is limited.
- To install Kaspersky applications remotely on client devices managed by the virtual Administration Server, you must make sure that Network Agent is installed on one of the client devices, in order to ensure communication with the virtual Administration Server. Upon first connection to the virtual Administration Server, the device is automatically assigned as a distribution point, thus functioning as a connection gateway between the client devices and the virtual Administration Server.
- A virtual Server can poll the network only through distribution points.
- To restart a malfunctioning virtual Server, Kaspersky Security Center Linux restarts the primary Administration Server and all virtual Administration Servers.
- Users created on a virtual Server cannot be assigned a role on the Administration Server.

The administrator of a virtual Administration Server has all privileges on this particular virtual Server.

# Web Server

Kaspersky Security Center *Web Server* (hereinafter also referred to as *Web Server*) is a component of Kaspersky Security Center that is installed together with Administration Server. Web Server is designed for transmission, over a network, of stand-alone installation packages, and files from a shared folder.

When you create a stand-alone installation package, it is automatically published on Web Server. The link for downloading the stand-alone package is displayed in the list of created stand-alone installation packages. If necessary, you can cancel publication of the stand-alone package or you can publish it on Web Server again.

The shared folder is used for storage of information that is available to all users whose devices are managed through Administration Server. If a user has no direct access to the shared folder, he or she can be given information from that folder by means of Web Server.

To provide users with information from a shared folder by means of Web Server, the administrator must create a subfolder named "public" in the shared folder and paste the relevant information into it.

The syntax of the information transfer link is as follows:

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

where:

- `<Web Server name>` is the name of Kaspersky Security Center Web Server.
- `<HTTPS port>` is an HTTPS port of Web Server that has been defined by the Administrator. The HTTPS port can be set in the **Web Server** section of the properties window of Administration Server. The default port number is 8061.
- `<object>` is the subfolder or file to which the user has access.

The administrator can send the new link to the user in any convenient way, such as by email.

By using this link, the user can download the required information to a local device.

# Kaspersky Security Center Linux Web Server

Kaspersky Security Center Linux Web Server (hereinafter referred to as Web Server) is a component of Kaspersky Security Center Linux. Web Server is designed for publishing stand-alone installation packages and files from the shared folder.

Installation packages that have been created are published on Web Server automatically and then removed after the first download. The administrator can send the new link to the user in any convenient way, such as by email.

By clicking the link, the user can download the required information to a mobile device.

### Web Server settings

If fine-tuning of Web Server is required, its properties allow you to change ports for HTTP (8060) and HTTPS (8061). In addition to changing ports, you can replace the server certificate for HTTPS and change the FQDN of Web Server for HTTP.

### Web Server settings on a connection gateway

A separate Web Server service is implemented on a distribution point in a connection gateway mode, which allows working with mobile devices connected to Kaspersky Security Center Linux. This service is responsible for transferring app installation packages and device management profiles to devices without directly connecting them to the Administration Server. Files are transferred as the service processes HTTP/HTTPS file requests on a connection gateway.

The Web Server service on a connection gateway is installed together with Network Agent Linux. To use this functionality, you must assign a device that will act as a distribution point in a connection gateway mode to be used as Web Server, and then specify the corresponding settings. For detailed information on configuring Web Server settings on a connection gateway, refer to the Kaspersky Secure Mobility Management Help.

## Network Agent

Interaction between Administration Server and devices is performed by the *Network Agent* component of Kaspersky Security Center Linux. Network Agent must be installed on all devices on which Kaspersky Security Center Linux is used to manage Kaspersky applications.

A device that has Network Agent installed is called a *managed device* or *device*. You can download the installation package for Network Agent from the following sources:

- Administration Server storage (you must have Administration Server installed)
- Kaspersky website

Network Agent for Linux is installed on a device as a service, with the following set of attributes:

- The name "Kaspersky Network Agent"
- Set to start automatically when the operating system starts
- Using the root account

Network Agent for Windows is installed on a device as a service, with the following set of attributes:

- The name "Kaspersky Security Center Network Agent"
- Set to start automatically when the operating system starts
- Using the LocalSystem account

Network Agent for macOS is installed on a device as a service, with the following set of attributes:

- The name "com.kaspersky.klnagent.core"
- Set to start automatically when the operating system starts
- Using the root account

The names of the service processes:

- For Linux:
  - klnagent64.service (for a 64-bit operating system)
  - klnagent.service (for a 32-bit operating system)
- For Windows:
  - klnagent
- For macOS:
  - com.kaspersky.klnagent

By default, Network Agent is installed in the following locations:

- For Linux:
  - 32-bit systems: /opt/kaspersky/klnagent/
  - 64-bit systems: /opt/kaspersky/klnagent64/
- For Windows:
  - 32-bit systems: C:\Program Files\Kaspersky Lab\NetworkAgent
  - 64-bit systems: C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
- For macOS:
  - 64-bit systems: /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

For Windows devices, you can specify a different folder for the installation of Network Agent in the settings of the installation package. However, for Linux devices, Network Agent can only be installed in the default directory.

The Network Agent installation folder also contains utilities for managing and diagnosing the operation of Network Agent, such as the klmover and klnagchk utilities.

When you install Administration Server, the server version of Network Agent is automatically installed together with Administration Server. Nevertheless, to manage the Administration Server device as any other managed device, install Network Agent for Linux on the Administration Server device. In this case, Network Agent for Linux is installed and works independently from the server version of Network Agent that you installed together with Administration Server.

Network Agent synchronizes the managed device with the Administration Server. We recommend that you set the synchronization interval (also referred to as the *heartbeat*) to 15 minutes per 10,000 managed devices.

# Administration groups

An *administration group* (hereinafter also referred to as *group*) is a logical set of managed devices combined on the basis of a specific trait for the purpose of managing the grouped devices as a single unit within Kaspersky Security Center Linux.

All managed devices within an administration group are configured to do the following:

- Use the same application settings (which you can specify in group policies).
- Use a common operating mode for all applications through the creation of group tasks with specified settings. Examples of group tasks include creating and installing a common installation package, updating the application databases and modules, scanning the device on demand, and enabling real-time protection.

A managed device can belong to only one administration group.

You can create hierarchies that have any degree of nesting for Administration Servers and groups. A single hierarchy level can include secondary and virtual Administration Servers, groups, and managed devices. You can move devices from one group to another without physically moving them. For example, if a worker's position in the enterprise changes from that of accountant to developer, you can move this worker's device from the Accountants administration group to the Developers administration group. Thereafter, the device will automatically receive the application settings required for developers.

# Managed device

A *managed device* is a device running Linux, Windows, or macOS and which has Network Agent installed. You can manage such devices by creating tasks and policies for applications installed on these devices. You can also receive reports from managed devices.

You can make a managed device function as a distribution point and as a connection gateway.

A device can be managed by only one Administration Server. The number of devices that can be managed by one Administration Server depends on configuration of the device that hosts the Administration Server and on DBMS restrictions.

# Unassigned device

An *unassigned device* is a device on the network that has not been included in any administration group. You can perform some actions on unassigned devices, for example, move them to administration groups or install applications on them.

When a new device is discovered on your network, this device goes to the **Unassigned devices** administration group. You can configure rules for devices to be moved automatically to other administration groups after the devices are discovered.

# Administrator's workstation

Devices on which Kaspersky Security Center Web Console Server is installed are referred to as *administrator's workstations*. Administrators can use these devices for centralized remote management of Kaspersky applications installed on client devices.

There are no restrictions on the number of administrator's workstations. From any administrator's workstation, you can manage administration groups of several Administration Servers on the network at once. You can connect an administrator's workstation to an Administration Server (physical or virtual) of any level of the hierarchy.

You can include an administrator's workstation in an administration group as a client device.

Within the administration groups of any Administration Server, the same device can function as an Administration Server client, an Administration Server, or an administrator's workstation.

# Management web plug-in

A special component—the *management web plug-in*—is used for remote administration of Kaspersky software by means of Kaspersky Security Center Web Console. Hereinafter, a management web plug-in is also referred to as a *management plug-in*. A management plug-in is an interface between Kaspersky Security Center Web Console and a specific Kaspersky application. With a management plug-in, you can configure tasks and policies for the application.

You can download management web plug-ins from the Kaspersky website.

The management plug-in provides the following:

- Interface for creating and editing application tasks and settings
- Interface for creating and editing policies and policy profiles for remote and centralized configuration of Kaspersky applications and devices
- Transmission of events generated by the application
- Kaspersky Security Center Web Console functions for displaying operational data and events of the application, and statistics relayed from client devices

# Policies

A *policy* is a set of Kaspersky application settings that are applied to an administration group and its subgroups. You can install several Kaspersky applications on the devices of an administration group. Kaspersky Security Center provides a single policy for each Kaspersky application in an administration group. A policy has one of the following statuses:

The status of the policy

| State | Description |
|---|---|
| Active | The current policy that is applied to the device. Only one policy may be active for a Kaspersky application in each administration group. Devices apply the settings values of an active policy for a Kaspersky application. |
| Inactive | A policy that is not currently applied to a device. |
| Out-of-office | If this option is selected, the policy becomes active when the device leaves the corporate network. |

Policies function according to the following rules:

- Multiple policies with different values can be configured for a single application.
- Only one policy can be active for the current application.
- A policy can have child policies.

Generally, you can use policies as preparations for emergency situations, such as a virus attack. For example, if there is an attack via flash drives, you can activate a policy that blocks access to flash drives. In this case, the current active policy automatically becomes inactive.

In order to prevent maintaining multiple policies, for example, when different occasions assume changing of several settings only, you may use policy profiles.

A *policy profile* is a named subset of policy settings values that replaces the settings values of a policy. A policy profile affects the effective settings formation on a managed device. *Effective settings* are a set of policy settings, policy profile settings, and local application settings that are currently applied for the device.

Policy profiles function according to the following rules:

- A policy profile takes effect when a specific activation condition occurs.
- Policy profiles contain values of settings that differ from the policy settings.
- Activation of a policy profile changes the effective settings of the managed device.
- A policy can include a maximum of 100 policy profiles.

# Policy profiles

Sometimes it may be necessary to create several instances of a single policy for different administration groups; you might also want to modify the settings of those policies centrally. These instances might differ by only one or two settings. For example, all the accountants in an enterprise work under the same policy—but senior accountants are allowed to use flash drives, while junior accountants are not. In this case, applying policies to devices only through the hierarchy of administration groups can be inconvenient.

To help you avoid creating several instances of a single policy, Kaspersky Security Center Linux enables you to create *policy profiles*. Policy profiles are necessary if you want devices within a single administration group to run under different policy settings.

A policy profile is a named subset of policy settings. This subset is distributed on target devices together with the policy, supplementing it under a specific condition called the *profile activation condition*. Profiles only contain settings that differ from the "basic" policy, which is active on the managed device. Activation of a profile modifies the settings of the "basic" policy that were initially active on the device. The modified settings take values that have been specified in the profile.

# Tasks

Kaspersky Security Center Linux manages Kaspersky security applications installed on devices by creating and running *tasks*. Tasks are required for installing, launching, and stopping applications, scanning files, updating databases and software modules, and performing other actions on applications.

Tasks for a specific application can be created only if the management plug-in for that application is installed.

Tasks can be performed on the Administration Server and on devices.

The following tasks are performed on the Administration Server:

- Automatic distribution of reports
- Downloading of updates to the repository of the Administration Server
- Backup of Administration Server data
- Maintenance of the database

The following types of tasks are performed on devices:

- *Local tasks*—Tasks that are performed on a specific device

  Local tasks can be modified either by the administrator, by using Kaspersky Security Center Web Console, or by the user of a remote device (for example, through the security application interface). If a local task has been modified simultaneously by the administrator and the user of a managed device, the changes made by the administrator will take effect because they have a higher priority.

- *Group tasks*—Tasks that are performed on all devices of a specific group

  Unless otherwise specified in the task properties, a group task also affects all subgroups of the selected group. A group task also affects (optionally) devices that have been connected to secondary and virtual Administration Servers deployed in the group or any of its subgroups.

- *Global tasks*—Tasks that are performed on a set of devices, regardless of whether they are included in any group

For each application, you can create any number of group tasks, global tasks, or local tasks.

You can make changes to the settings of tasks, view the progress of tasks, and copy, export, import, and delete tasks.

A task is started on a device only if the application for which the task was created is running.

Results of tasks are saved in the Syslog event log and the Kaspersky Security Center Linux event log, both centrally on the Administration Server and locally on each device.

Do not include private data in task settings. For example, avoid specifying the domain administrator password.

# Task scope

The *scope of a task* is the set of devices on which the task is performed. The types of scope are as follows:

- For a *local task*, the scope is the device itself.
- For an *Administration Server task*, the scope is the Administration Server.
- For a *group task*, the scope is the list of devices included in the group.

When creating a *global task*, you can use the following methods to specify its scope:

- Specifying certain devices manually.

  You can use an IP address (or IP range) or DNS name as the device address. You can also select networked devices detected by Administration Server.

- Importing a list of devices from a .txt file with the device addresses to be added (each address must be placed on an individual line).

  If you import a list of devices from a file or create a list manually, and if devices are identified by their names, the list can only contain devices for which information has already been entered into the Administration Server database. Moreover, the information must have been entered when those devices were connected or during device discovery.

- Specifying a device selection.

  Over time, the scope of a task changes as the set of devices included in the selection change. A selection of devices can be made on the basis of device attributes, including software installed on a device, and on the basis of tags assigned to devices. Device selection is the most flexible way to specify the scope of a task.

  Tasks for device selections are always run on a schedule by the Administration Server. These tasks cannot be run on devices that lack connection to the Administration Server. Tasks whose scope is specified by using other methods are run directly on devices and therefore do not depend on the device connection to the Administration Server.

  Tasks for device selections are not run on the local time of a device; instead, they are run on the local time of the Administration Server. Tasks whose scope is specified by using other methods are run on the local time of a device.

# How local application settings relate to policies

You can use policies to set identical values of the application settings for all devices in a group.

The values of the settings that a policy specifies can be redefined for individual devices in a group by using local application settings. You can set only the values of settings that the policy allows to be modified, that is, the unlocked settings.

The value of a setting that the application uses on a client device is defined by the lock position (🔒) for that setting in the policy:

- If a setting modification is locked, the same value (defined in the policy) is used on all client devices.
- If a setting modification is unlocked, the application uses a local setting value on each client device instead of the value specified in the policy. The setting can then be changed in the local application settings.

This means that, when a task is run on a client device, the application applies settings that have been defined in two different ways:

- By task settings and local application settings, if the setting is not locked against changes in the policy.
- By the group policy, if the setting is locked against changes.

Local application settings are changed after the policy is first applied in accordance with the policy settings.

# Distribution point

*Distribution point* (previously known as update agent) is a device with Network Agent installed that is used for update distribution, remote installation of applications, and retrieval of information about networked devices.

> The features and use cases of Network Agent installed on a device used as a distribution point vary depending on the operating system.

A distribution point can perform the following functions:

- Distribute updates and installation packages received from the Administration Server to client devices within the group (including distribution through multicasting using UDP). Updates can be received either from the Administration Server or from Kaspersky update servers. In the latter case, an update task must be created for the distribution point.

  Distribution points accelerate update distribution and free up Administration Server resources.

- Distribute policies and group tasks through multicasting using UDP.

- Act as a gateway for connection to the Administration Server for devices in an administration group.

  If a direct connection between managed devices within the group and the Administration Server cannot be established, you can use the distribution point as a connection gateway to the Administration Server for this group. In this case, managed devices connect to the connection gateway, which in turn connects to the Administration Server.

  The presence of a distribution point that functions as connection gateway does not block the option of a direct connection between managed devices and the Administration Server. If the connection gateway is not available, but direct connection with the Administration Server is technically possible, managed devices are connected to the Administration Server directly.

- Poll the network to detect new devices and update information about existing ones. A distribution point can apply the same device discovery methods as the Administration Server.

- Perform remote installation of applications by Kaspersky and other software vendors, including installation on client devices without Network Agent.

  This feature allows you to remotely transfer Network Agent installation packages to client devices located on networks to which the Administration Server has no direct access.

- Act as a proxy server participating in Kaspersky Security Network (KSN).

  You can enable KSN proxy server on distribution point side to make the device act as a KSN proxy server. In this case, the KSN proxy service is run on the device.

Files are transmitted from the Administration Server to a distribution point over HTTP or, if SSL connection is enabled, over HTTPS. Using HTTP or HTTPS results in a higher level of performance, compared to SOAP, through cutting traffic.

Devices with Network Agent installed can be assigned distribution points either manually (by the administrator), or automatically (by the Administration Server). The full list of distribution points for specified administration groups is displayed in the report about the list of distribution points.

The scope of a distribution point is the administration group to which it has been assigned by the administrator, as well as its subgroups of all levels of embedding. If multiple distribution points have been assigned in the hierarchy of administration groups, Network Agent on the managed device connects to the nearest distribution point in the hierarchy.

If distribution points are assigned automatically by the Administration Server, it assigns them by broadcast domains, not by administration groups. This occurs when all broadcast domains are known. Network Agent exchanges messages with other Network Agents in the same subnet and then sends Administration Server information about itself and other Network Agents. Administration Server can use that information to group Network Agents by broadcast domains. Broadcast domains are known to Administration Server after more than 70% Network Agents in administration groups are polled. Administration Server polls broadcast domains every two hours. After distribution points are assigned by broadcast domains, they cannot be re-assigned by administration groups.

If the administrator manually assigns distribution points, they can be assigned to administration groups or network locations.

Network Agents with an active connection profile do not participate in broadcast domain detection.

Kaspersky Security Center Linux assigns each Network Agent a unique IP multicast address that differs from every other address. This allows you to avoid network overload that might occur due to IP overlaps. IP multicast addresses that were assigned in previous versions of the application will not be changed.

If two or more distribution points are assigned to a single network area or to a single administration group, one of them becomes the active distribution point, and the rest become standby distribution points. The active distribution point downloads updates and installation packages directly from the Administration Server, while standby distribution points receive updates from the active distribution point only. In this case, files are downloaded once from the Administration Server and then are distributed among distribution points. If the active distribution point becomes unavailable for any reason, one of the standby distribution points becomes active. The Administration Server automatically assigns a distribution point to act as standby.

The distribution point status (*Active*/*Standby*) is displayed with a check box in the klnagchk report.

A distribution point requires at least 4 GB of free disk space. If the free disk space of the distribution point is less than 2 GB, Kaspersky Security Center Linux creates a security issue with the *Warning* importance level. The security issue will be published in the device properties, in the **Security issues** section.

Running remote installation tasks on a device assigned as a distribution point requires additional free disk space. The volume of free disk space must exceed the total size of all installation packages to be installed.

Running any updating (patching) tasks and vulnerability fix tasks on a device assigned as a distribution point requires additional free disk space. The volume of free disk space must be at least twice the total size of all patches to be installed.

Devices functioning as distribution points must be protected, including physical protection, against any unauthorized access.

# Connection gateway

A *connection gateway* is a Network Agent acting in a special mode. A connection gateway accepts connections from other Network Agents and tunnels them to the Administration Server through its own connection with the Server. Unlike an ordinary Network Agent, a connection gateway waits for connections from the Administration Server rather than establishes connections to the Administration Server.

A connection gateway can receive connections from up to 10,000 devices.

You have two options for using connection gateways:

- We recommend that you install a connection gateway in a demilitarized zone (DMZ). For other Network Agents installed on out-of-office devices, you need to specially configure a connection to Administration Server through the connection gateway.

  A connection gateway does not in any way modify or process data that is transmitted from Network Agents to Administration Server. Moreover, it does not write this data into any buffer and therefore cannot accept data from a Network Agent and later forward it to Administration Server. If Network Agent attempts to connect to Administration Server through the connection gateway, but the connection gateway cannot connect to Administration Server, Network Agent perceives this as if Administration Server is inaccessible. All data remains on Network Agent (not on the connection gateway).

  A connection gateway cannot connect to Administration Server through another connection gateway. It means that Network Agent cannot simultaneously be a connection gateway and use a connection gateway to connect to Administration Server.

  All connection gateways are included in the list of distribution points in the Administration Server properties.

- You can also use connection gateways within the network. For example, automatically assigned distribution points also become connection gateways in their own scope. However, within an internal network, connection gateways do not provide considerable benefit. They reduce the number of network connections received by Administration Server, but do not reduce the volume of incoming data. Even without connection gateways, all devices could still connect to Administration Server.

# Virtual Administration Servers

On the basis of a physical Administration Server, multiple virtual Administration Servers can be created, which will be similar to secondary Administration Servers. Compared to the discretionary access model, which is based on access control lists (ACLs), the virtual Administration Server model is more functional and provides a larger degree of isolation. In addition to a dedicated structure of administration groups for assigned devices with policies and tasks, each virtual Administration Server features its own group of unassigned devices, own sets of reports, selected devices and events, installation packages, moving rules, etc. The functional scope of virtual Administration Servers can be used both by service providers (xSP) to maximize the isolation of customers, and by large-scale organizations with sophisticated workflows and numerous administrators.

Virtual Administration Servers are very similar to secondary Administration Servers, but with the following distinctions:

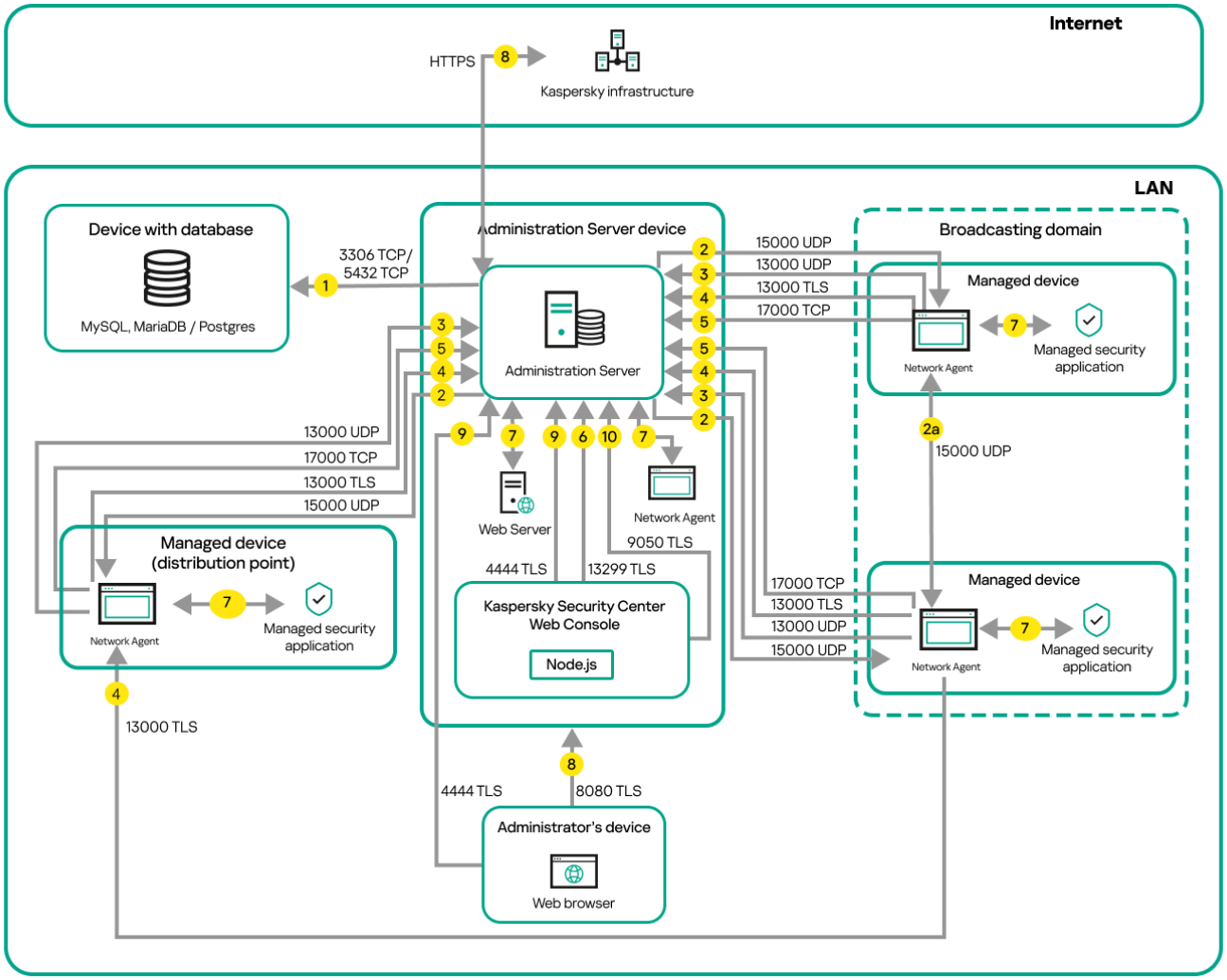
- A virtual Administration Server lacks most global settings and its own TCP ports.
- A virtual Administration Server has no secondary Administration Servers.
- A virtual Administration Server has no other virtual Administration Servers.
- A physical Administration Server views devices, groups, events, and objects on managed devices (items in Quarantine, applications registry, etc.) of all its virtual Administration Servers.
- A virtual Administration Server can only scan the network with distribution points connected.

# Schemas for data traffic and port usage

This section provides schemas for data traffic between Kaspersky Security Center Linux components, managed security applications, and external servers under various configurations. The schemas are provided with numbers for the ports that must be available on the local devices.

## Administration Server and managed devices on a local area network (LAN)

The figure below shows the traffic of the data if Kaspersky Security Center is deployed on a local area network (LAN) only.




Administration Server and managed devices on a local area network (LAN)

The figure shows how different managed devices connect to the Administration Server in different ways: directly or via a distribution point. Distribution points reduce the load on the Administration Server during update distribution and optimize network traffic. However, distribution points are only needed if the number of managed devices is large enough. If the number of managed devices is small, all the managed devices can receive updates from the Administration Server directly.

The arrows indicate the initiation of traffic: each arrow points from a device that initiates the connection to the device that "answers" the call. The number of the port and the name of the protocol used for data transfer are provided. Each arrow has a number label, and details about the corresponding data traffic are as follows:

1. Administration Server sends data to the database. If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 5432 for PostgreSQL Server or Postgres Pro Server). Please refer to the DBMS documentation for the relevant information.

2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000.

   Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

   If Administration Server does not have direct access to the managed devices, communication requests from Administration Server to these devices are not sent directly.

   2a. Network Agents on non-mobile managed devices exchange data about other Network Agents within the same broadcasting domain (the data is then sent to the Administration Server).

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.

4. The Administration Server receives connection from Network Agents and from secondary Administration Servers through TLS port 13000.

   If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-TLS port 14000. Kaspersky Security Center also supports connection of Network Agents through port 14000, although using TLS port 13000 is recommended.

5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the internet; in this case, the device sends the data to Kaspersky servers over the internet directly.

6. Kaspersky Security Center Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.

   The Identity and Access Manager (IAM) component connects to Administration Server through TLS port 13299.

7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.

8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

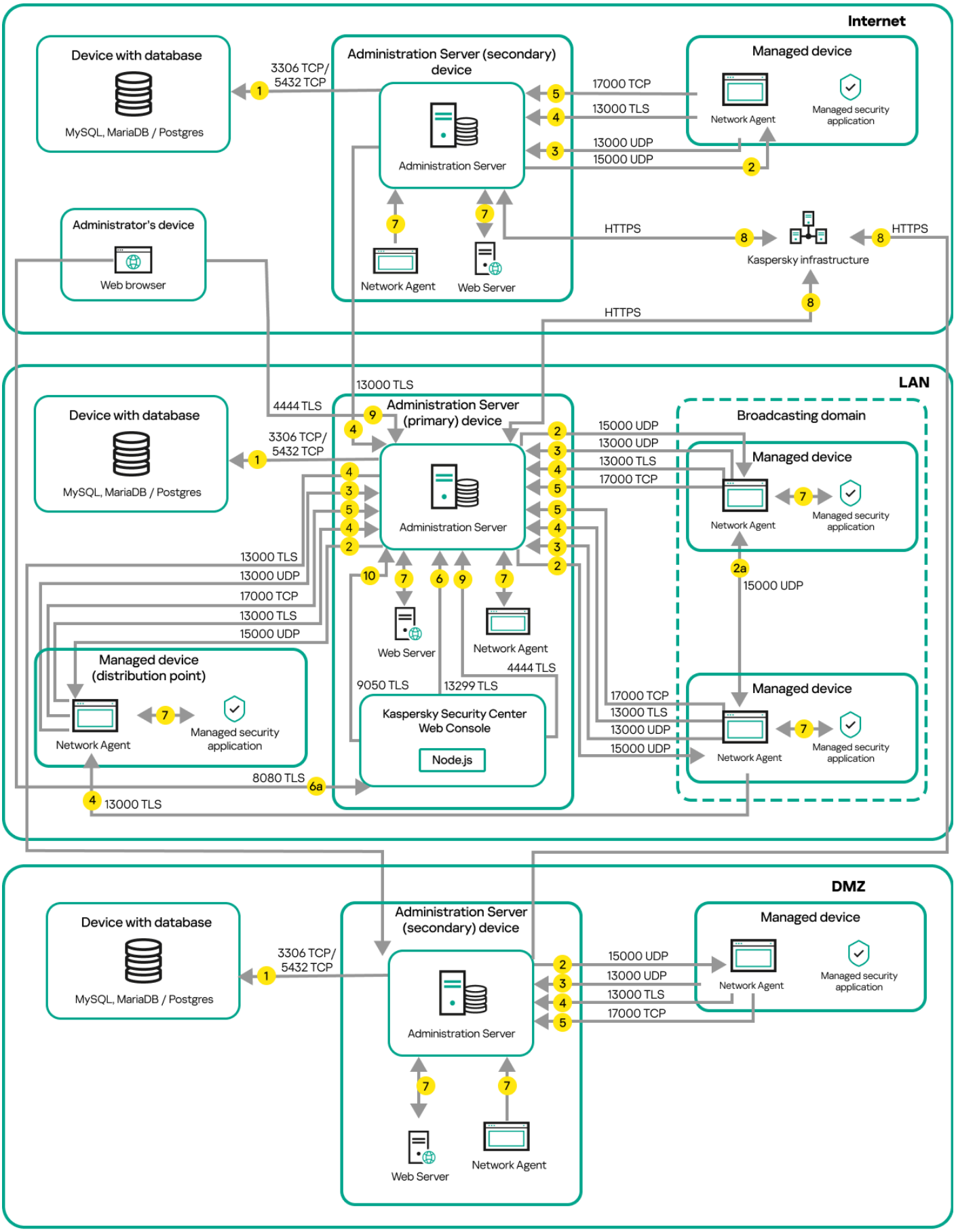
   If you do not want your Administration Server to have access to the internet, you must manage this data manually.

9. Kaspersky Security Center Web Console Server and the browser (used with Kaspersky Security Center Web Console) connect to Administration Server over the OpenID Connect authentication protocol through TLS port 4444.

10. Kaspersky Security Center Web Console Server connects to Administration Server through TLS port 9050.

# Primary Administration Server on LAN and two secondary Administration Servers

The figure below shows the hierarchy of Administration Servers: the primary Administration Server is on a local area network (LAN). A secondary Administration Server is in the demilitarized zone (DMZ); another secondary Administration Server is on the internet.




Hierarchy of Administration Servers: primary Administration Server and two secondary Administration Servers

The arrows indicate the initiation of traffic: each arrow points from a device that initiates the connection to the device that "answers" the call. The number of the port and the name of the protocol used for data transfer are provided. Each arrow has a number label, and details about the corresponding data traffic are as follows:

1. Administration Server sends data to the database. If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 5432 for PostgreSQL Server or Postgres Pro Server). Please refer to the DBMS documentation for the relevant information.

2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000.

   Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

   If Administration Server does not have direct access to the managed devices, communication requests from Administration Server to these devices are not sent directly.

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.

4. The Administration Server receives connection from Network Agents and from secondary Administration Servers through TLS port 13000.

   If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-TLS port 14000. Kaspersky Security Center Linux also supports connection of Network Agents through port 14000, although using TLS port 13000 is recommended.

5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the internet; in this case, the device sends the data to Kaspersky servers over the internet directly.

6. Kaspersky Security Center Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.

   The Identity and Access Manager (IAM) component connects to Administration Server through TLS port 13299.

   6a. Data from the browser, which is installed on a separate device of the administrator, is transferred to Kaspersky Security Center Web Console Server through TLS port 8080. The Kaspersky Security Center Web Console Server can be installed either on the Administration Server or on another device.

7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.

8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

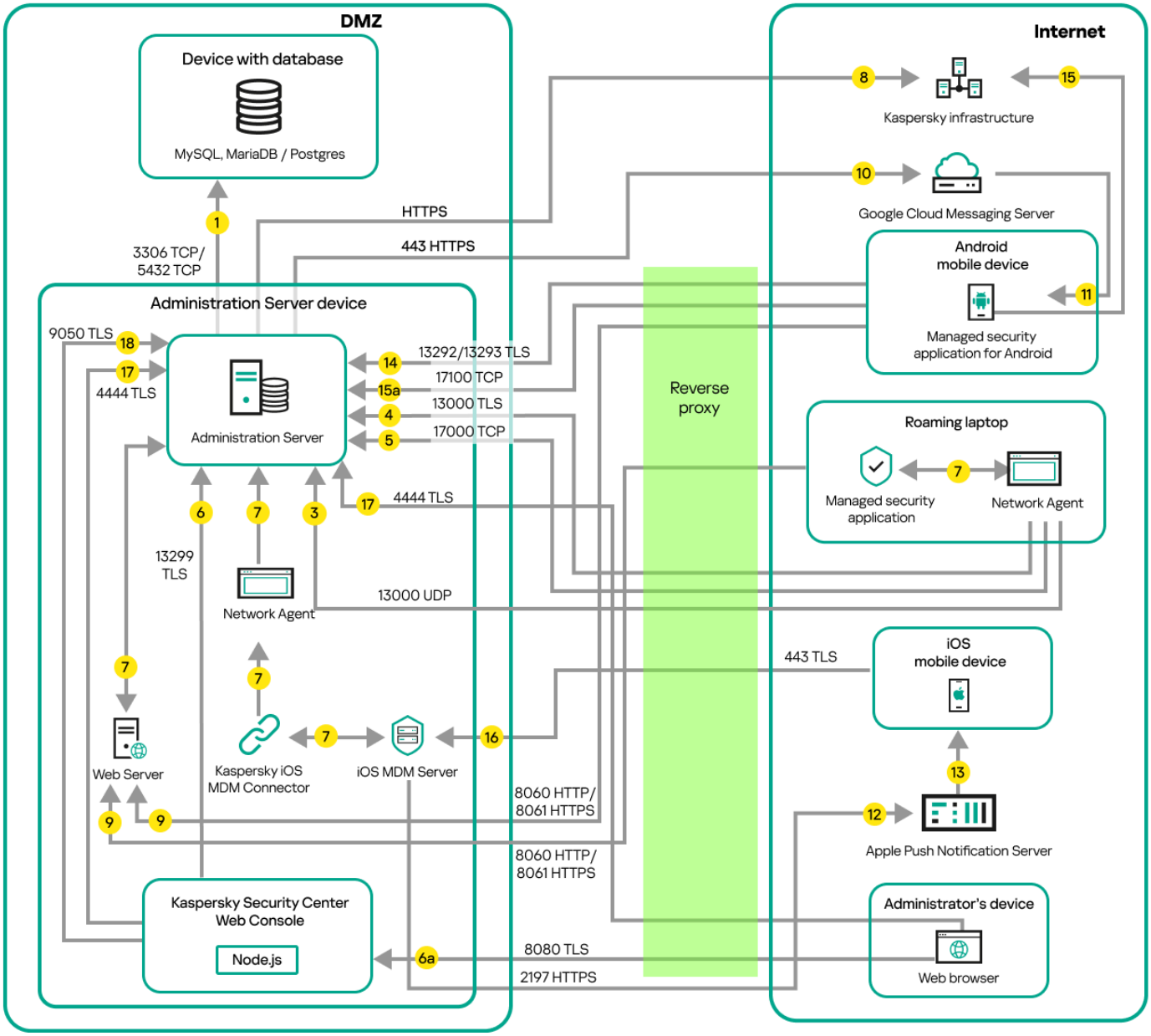
   If you do not want your Administration Server to have access to the internet, you must manage this data manually.

9. Kaspersky Security Center Web Console Server and the browser (used with Kaspersky Security Center Web Console) connect to Administration Server over the OpenID Connect authentication protocol through TLS port 4444.

10. Kaspersky Security Center Web Console Server connects to Administration Server through TLS port 9050.

# Administration Server on LAN, managed devices on internet, reverse proxy in use

The figure below shows data traffic if the Administration Server is on a local area network (LAN) and the managed devices are on the internet. In this figure, a reverse proxy of your choice is in use. Refer to the documentation of the application for details.




Administration Server on a local area network; managed devices connect to the Administration Server through a reverse proxy

This deployment scheme is recommended if you do not want the mobile devices to connect to the Administration Server directly and do not want to assign a connection gateway in the DMZ.

The arrows indicate the initiation of traffic: each arrow points from a device that initiates the connection to the device that "answers" the call. The number of the port and the name of the protocol used for data transfer are provided. Each arrow has a number label, and details about the corresponding data traffic are as follows:

1. Administration Server sends data to the database. If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 5432 for PostgreSQL Server or Postgres Pro Server). Please refer to the DBMS documentation for the relevant information.

2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000.

   Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

   If Administration Server does not have direct access to the managed devices, communication requests from Administration Server to these devices are not sent directly.

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.

4. The Administration Server receives connection from Network Agents and from secondary Administration Servers through TLS port 13000.

   If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-TLS port 14000. Kaspersky Security Center Linux also supports connection of Network Agents through port 14000, although using TLS port 13000 is recommended.

5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the internet; in this case, the device sends the data to Kaspersky servers over the internet directly.

6. Kaspersky Security Center Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.

   The Identity and Access Manager (IAM) component connects to Administration Server through TLS port 13299.

   6a. Data from the browser, which is installed on a separate device of the administrator, is transferred to Kaspersky Security Center Web Console Server through TLS port 8080. The Kaspersky Security Center Web Console Server can be installed either on the Administration Server or on another device.

7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.

8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

   If you do not want your Administration Server to have access to the internet, you must manage this data manually.

9. Requests for packages from managed devices, including mobile devices, are transferred to the Web Server, which is on the same device as the Administration Server.

10. For Android mobile devices only: data from the Administration Server is transferred to Google servers. This connection is used to notify Android mobile devices that they are required to connect to the Administration Server. Then push notifications are sent to the mobile devices.

11. For Android mobile devices only: push notifications from Google servers are sent to the mobile device. This connection is used to notify mobile devices that they are required to connect to the Administration Server.

12. For iOS mobile devices only: data from the iOS MDM Server is transferred to Apple Push Notification servers. Then push notifications are sent to the mobile devices.

13. For iOS mobile devices only: push notifications are sent from Apple servers to the mobile device. This connection is used to notify iOS mobile devices that they are required to connect to the iOS MDM Server.

14. For mobile devices only: data from the managed application is transferred to the Administration Server (or to the connection gateway) through TLS port 13292 / 13293—directly or through a reverse proxy.

15. For mobile devices only: data from the mobile device is transferred to the Kaspersky infrastructure.

    If a mobile device does not have internet access, the data is transferred to Administration Server through port 17100, and the Administration Server sends it to the Kaspersky infrastructure. However, this scenario applies very rarely.

16. For iOS mobile devices only: data from the mobile device is transferred through TLS port 443 to the iOS MDM Server, which is on the same device as the Administration Server or on the connection gateway.

17. Kaspersky Security Center Web Console Server and the browser (used with Kaspersky Security Center Web Console) connect to Administration Server over the OpenID Connect authentication protocol through TLS port 4444.

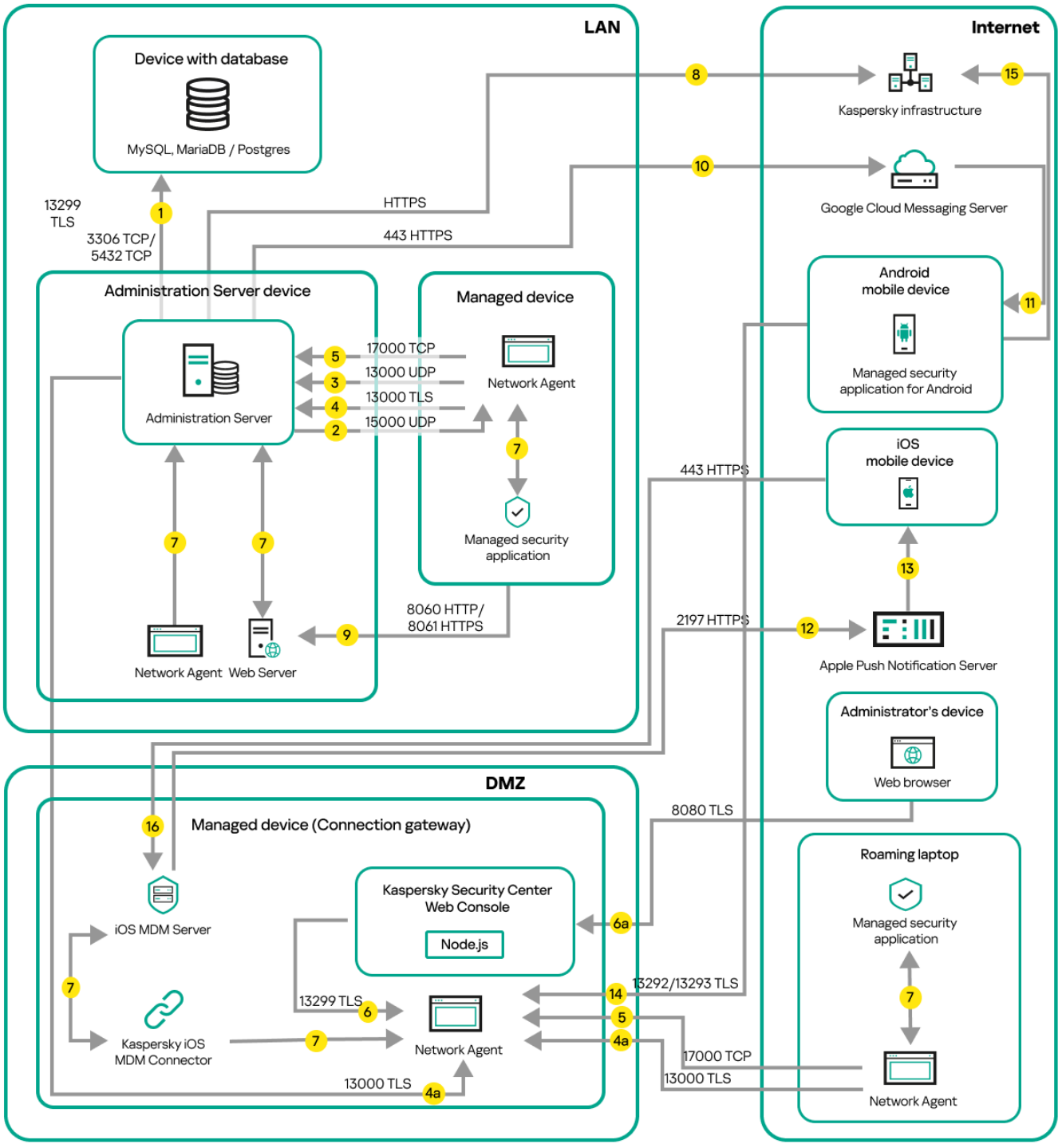
18. Kaspersky Security Center Web Console Server connects to Administration Server through TLS port 9050.

# Administration Server on LAN, managed devices on internet, connection gateway in use

The figure below shows data traffic if the Administration Server is on a local area network (LAN) and the managed devices are on the internet. A connection gateway is in use.

This deployment scheme is recommended if you do not want the managed devices to connect to the Administration Server directly and do not want to use a reverse proxy or corporate firewall.

For this deployment scheme, domain authentication (single sign-on) provided by Identity and Access Manager (IAM) is not supported.




Managed mobile devices connected to the Administration Server through a connection gateway

In this figure, the managed devices are connected to the Administration Server through a connection gateway that is located in the DMZ. No reverse proxy and corporate firewall is in use.

The arrows indicate the initiation of traffic: each arrow points from a device that initiates the connection to the device that "answers" the call. The number of the port and the name of the protocol used for data transfer are provided. Each arrow has a number label, and details about the corresponding data traffic are as follows:

1. Administration Server sends data to the database. If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 5432 for PostgreSQL Server or Postgres Pro Server). Please refer to the DBMS documentation for the relevant information.

2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000.

   Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

   If Administration Server does not have direct access to the managed devices, communication requests from Administration Server to these devices are not sent directly.

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.

4. The Administration Server receives connection from Network Agents and from secondary Administration Servers through TLS port 13000.

   If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-TLS port 14000. Kaspersky Security Center Linux also supports connection of Network Agents through port 14000, although using TLS port 13000 is recommended.

   4a. A connection gateway in DMZ also receives connection from the Administration Server through TLS port 13000. Because a connection gateway in DMZ cannot reach the Administration Server's ports, the Administration Server creates and maintains a permanent signal connection with a connection gateway. The signal connection is not used for data transfer; it is only used for sending an invitation to the network interaction. When the connection gateway needs to connect to the Server, it notifies the Server through this signal connection, and then the Server creates the required connection for data transfer.

   Out-of-office devices connect to the connection gateway through TLS port 13000 as well.

5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the internet; in this case, the device sends the data to Kaspersky servers over the internet directly.

6. Kaspersky Security Center Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.

   6a. Data from the browser, which is installed on a separate device of the administrator, is transferred to Kaspersky Security Center Web Console Server through TLS port 8080. The Kaspersky Security Center Web Console Server can be installed either on the Administration Server or on another device.

7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.

8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

   If you do not want your Administration Server to have access to the internet, you must manage this data manually.

9. Requests for packages from managed devices, including mobile devices, are transferred to the Web Server, which is on the same device as the Administration Server.

10. For Android mobile devices only: data from the Administration Server is transferred to Google servers. This connection is used to notify Android mobile devices that they are required to connect to the Administration Server. Then push notifications are sent to the mobile devices.

11. For Android mobile devices only: push notifications from Google servers are sent to the mobile device. This connection is used to notify mobile devices that they are required to connect to the Administration Server.

12. For iOS mobile devices only: data from the iOS MDM Server is transferred to Apple Push Notification servers. Then push notifications are sent to the mobile devices.

13. For iOS mobile devices only: push notifications are sent from Apple servers to the mobile device. This connection is used to notify iOS mobile devices that they are required to connect to the iOS MDM Server.

14. For mobile devices only: data from the managed application is transferred to the Administration Server (or to the connection gateway) through TLS port 13292 / 13293—directly or through a reverse proxy.

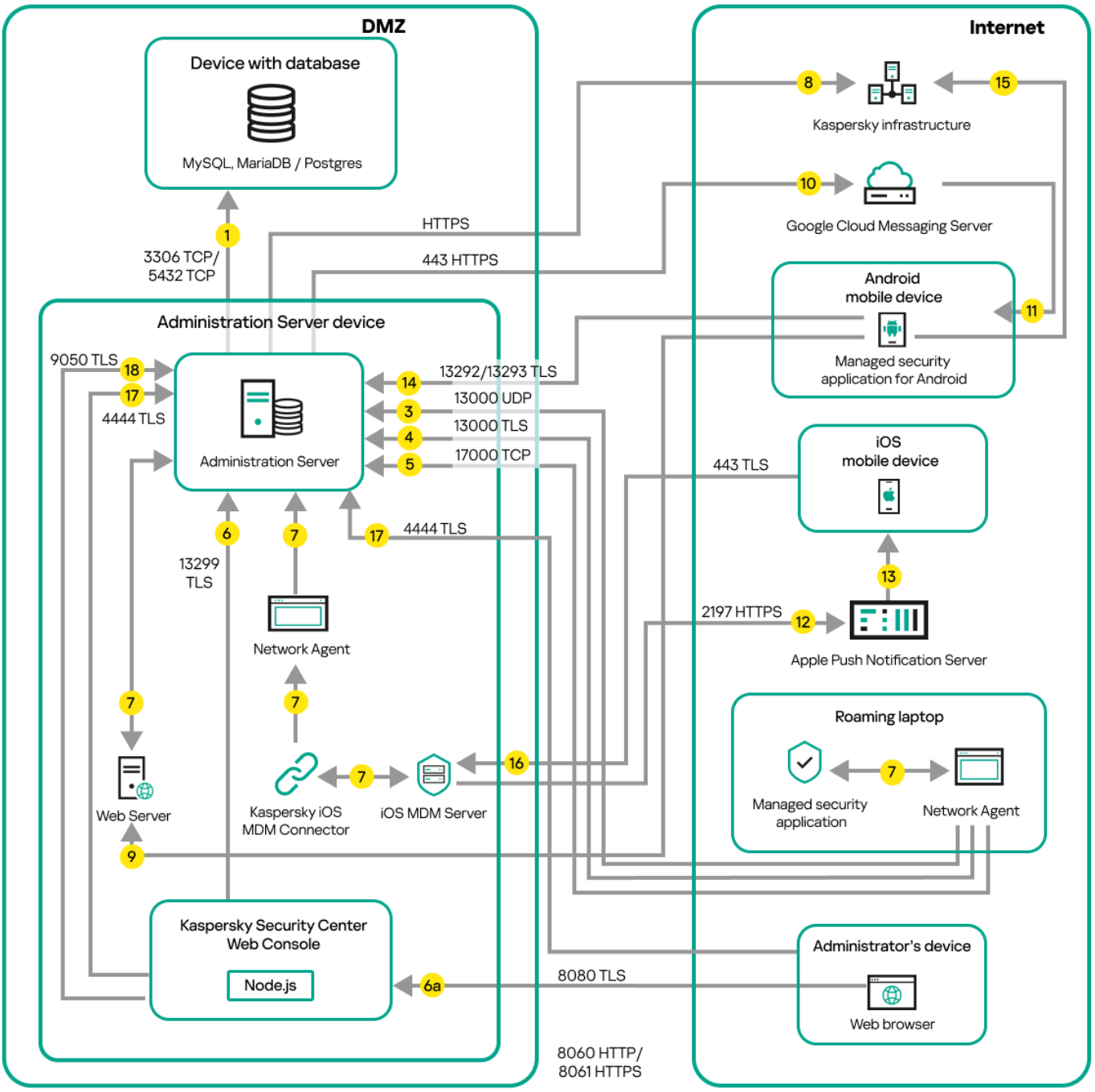
15. For mobile devices only: data from the mobile device is transferred to the Kaspersky infrastructure.

    If a mobile device does not have internet access, the data is transferred to Administration Server through port 17100, and the Administration Server sends it to the Kaspersky infrastructure. However, this scenario applies very rarely.

16. For iOS mobile devices only: data from the mobile device is transferred through TLS port 443 to the iOS MDM Server, which is on the same device as the Administration Server or on the connection gateway.

# Administration Server in DMZ, managed devices on internet

The figure below shows data traffic if the Administration Server is in the demilitarized zone (DMZ) and the managed devices are on the internet.




Administration Server in DMZ, managed mobile devices on the internet

In this figure, a connection gateway is not in use: the mobile devices connect to the Administration Server directly.

The arrows indicate the initiation of traffic: each arrow points from a device that initiates the connection to the device that "answers" the call. The number of the port and the name of the protocol used for data transfer are provided. Each arrow has a number label, and details about the corresponding data traffic are as follows:

1. Administration Server sends data to the database. If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 5432 for PostgreSQL Server or Postgres Pro Server). Please refer to the DBMS documentation for the relevant information.

2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000.

   Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

   If Administration Server does not have direct access to the managed devices, communication requests from Administration Server to these devices are not sent directly.

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.

4. The Administration Server receives connection from Network Agents and from secondary Administration Servers through TLS port 13000.

   If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-TLS port 14000. Kaspersky Security Center Linux also supports connection of Network Agents through port 14000, although using TLS port 13000 is recommended.

5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the internet; in this case, the device sends the data to Kaspersky servers over the internet directly.

6. Kaspersky Security Center Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.

   The Identity and Access Manager (IAM) component connects to Administration Server through TLS port 13299.

   6a. Data from the browser, which is installed on a separate device of the administrator, is transferred to Kaspersky Security Center Web Console Server through TLS port 8080. The Kaspersky Security Center Web Console Server can be installed either on the Administration Server or on another device.

7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.

8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

   If you do not want your Administration Server to have access to the internet, you must manage this data manually.

9. Requests for packages from managed devices are transferred to the Web Server, which is on the same device as the Administration Server.

10. For Android mobile devices only: data from the Administration Server is transferred to Google servers. This connection is used to notify Android mobile devices that they are required to connect to the Administration Server. Then push notifications are sent to the mobile devices. FCM service also runs on 443 HTTPS port.

11. For Android mobile devices only: push notifications from Google servers are sent to the mobile device. This connection is used to notify mobile devices that they are required to connect to the Administration Server.

12. For iOS mobile devices only: data from the iOS MDM Server is transferred to Apple Push Notification servers. Then push notifications are sent to the mobile devices.

13. For iOS mobile devices only: push notifications are sent from Apple servers to the mobile device. This connection is used to notify iOS mobile devices that they are required to connect to the iOS MDM Server.

14. For mobile devices only: data from the managed application is transferred to the Administration Server (or to the connection gateway) through TLS port 13292 / 13293—directly or through a reverse proxy.

15. For mobile devices only: data from the mobile device is transferred to the Kaspersky infrastructure.

    If a mobile device does not have internet access, the data is transferred to Administration Server through port 17100, and the Administration Server sends it to the Kaspersky infrastructure. However, this scenario applies very rarely.

16. For iOS mobile devices only: data from the mobile device is transferred through TLS port 443 to the iOS MDM Server, which is on the same device as the Administration Server or on the connection gateway.

17. Kaspersky Security Center Web Console Server and the browser (used with Kaspersky Security Center Web Console) connect to Administration Server over the OpenID Connect authentication protocol through TLS port 4444.

18. Kaspersky Security Center Web Console Server connects to Administration Server through TLS port 9050.

# Interaction of Kaspersky Security Center Linux components and security applications: more information

This section provides the schemas for interaction of Kaspersky Security Center Linux components and managed security applications. The schemas provide the numbers of the ports that must be available and the names of the processes that open those ports.

## Conventions used in interaction schemas

The following table provides the conventions used across the schemas.

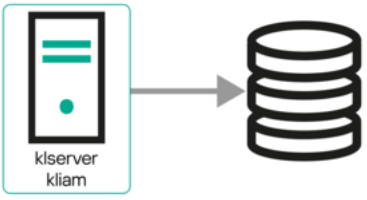
Document conventions

| Icon | Value |
|---|---|
|  | Administration Server |
|  | Secondary Administration Server |
|  | DBMS |

| | |
|---|---|
|  | Client device (that has Network Agent and an application from Kaspersky Endpoint Security family installed, or has a different security application installed that Kaspersky Security Center Linux can manage) |
|  | Connection gateway |
|  | Distribution point |
|  | Browser on the user's device |
|   | Process running on the device and opening a port |
|   | Port and its number |
|  | TCP traffic (the arrow direction shows the traffic flow direction) |
|  | UDP traffic (the arrow direction shows the traffic flow direction) |
|  | DBMS transport |
|  | DMZ boundary |

# Administration Server and DBMS

The data of the Administration Server and Identity and Access Manager (IAM) are stored in separate databases within the same DBMS.



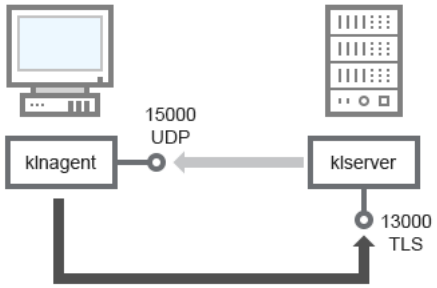

Administration Server, Identity and Access Manager, and DBMS

If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MariaDB). Please refer to the DBMS documentation for the relevant information.
The port for connecting IAM to the DBMS is specified by a user during Kaspersky Security Center Linux installation.

The Administration Server does not automatically remove the Administration Server database and the IAM database when uninstalling or moving the server to another device. If necessary, you must remove the databases manually.

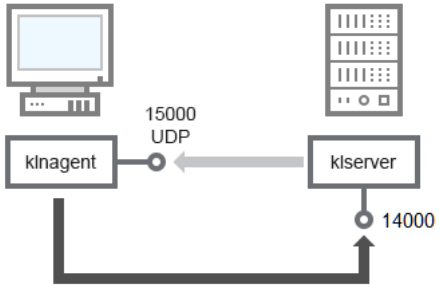
# Administration Server and client device: Managing the security application

The Administration Server receives connection from Network Agents via TLS port 13000 (see figure below).




Administration Server and client device: managing the security application, connection via port 13000 (recommended)

If you used an earlier version of Kaspersky Security Center Linux, the Administration Server on your network can receive connections from Network Agents via non-SSL port 14000 (see figure below). Kaspersky Security Center Linux also supports connection of Network Agents via port 14000, although using SSL port 13000 is recommended.




Administration Server and client device: managing the security application, connection via port 14000 (lower security)

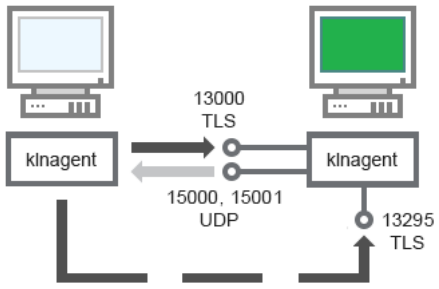
For clarifications of schemas, see the table below.

Administration Server and client device: Managing the security application (traffic)

| Device | Port number | Name of the process that opens the port | Protocol | Port purpose |
|---|---|---|---|---|
| Network Agent | 15000 | klnagent | UDP | Multicasting for Network Agents |
| Administration Server | 13000 | klserver | TCP (TLS) | Receiving connections from Network Agents |
| Administration Server | 14000 | klserver | TCP | Receiving connections from Network Agents |

# Upgrading software on a client device through a distribution point

The client device connects to the distribution point via port 13000 and, if you are using the distribution point as a push server, also via port 13295; the distribution point multicasts to Network Agents via port 15000 (see figure below). Updates and installation packages are received from a distribution point via port 15001.




Upgrading software on a client device through a distribution point

For schema clarifications, see the table below.

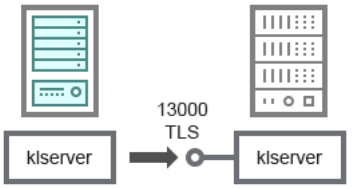
Upgrading software through a distribution point (traffic)

| Device | Port number | Name of the process that opens the port | Protocol | Port purpose |
|---|---|---|---|---|
| Network Agent | 15000 | klnagent | UDP | Multicasting for Network Agents |
| Network Agent | 15001 | klnagent | UDP | Receiving updates and installation packages from a distribution point |
| Distribution point | 13000 | klnagent | TCP (TLS) | Receiving connections from Network Agents |
| Distribution point | 13295 | klnagent | TCP (TLS) | Receiving connections from client devices (server push) |

# Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server

The schema (see figure below) shows how to use port 13000 to ensure interaction between Administration Servers combined into a hierarchy.

Subsequently, when the Administration Servers are combined into a hierarchy, you will be able to administer both of them by using Kaspersky Security Center Web Console connected to the primary Administration Server. Therefore, the accessibility of port 13299 of the primary Administration Server is the only prerequisite.



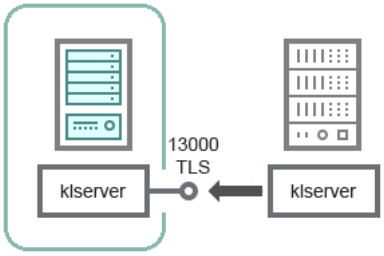

Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server

For schema clarifications, see the table below.

Hierarchy of Administration Servers (traffic)

| Device | Port number | Name of the process that opens the port | Protocol | Port purpose |
|---|---|---|---|---|
| Primary Administration Server | 13000 | klserver | TCP (TLS) | Receiving connections from secondary Administration Servers |

# Hierarchy of Administration Servers with a secondary Administration Server in DMZ




Hierarchy of Administration Servers with a secondary Administration Server in DMZ

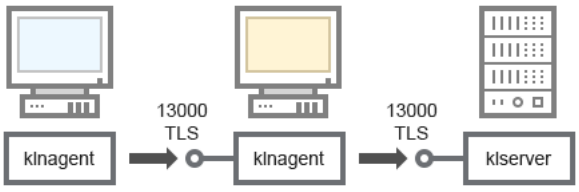
The schema shows a hierarchy of Administration Servers in which the secondary Administration Server located in DMZ receives a connection from the primary Administration Server (see the table below for schema clarifications). When combining two Administration Servers into a hierarchy, make sure that port 13299 is accessible on both Administration Servers. Kaspersky Security Center Web Console connects to Administration Server through port 13299.

Subsequently, when the Administration Servers are combined into a hierarchy, you will be able to administer both of them by using Kaspersky Security Center Web Console connected to the primary Administration Server. Therefore, the accessibility of port 13299 of the primary Administration Server is the only prerequisite.

Hierarchy of Administration Servers with a secondary Administration Server in DMZ (traffic)

| Device | Port number | Name of the process that opens the port | Protocol | Port purpose |
|---|---|---|---|---|
| Secondary Administration Server | 13000 | klserver | TCP (TLS) | Receiving connections from the primary Administration Server |

# Administration Server, a connection gateway in a network segment, and a client device



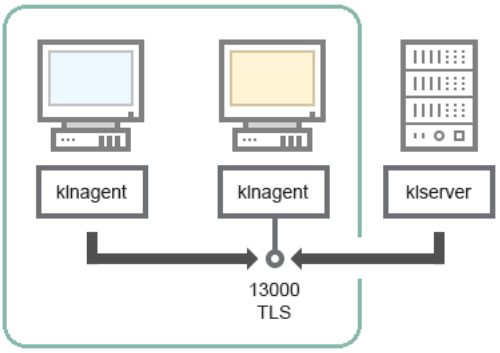

Administration Server, a connection gateway in a network segment, and a client device

For schema clarifications, see the table below.

Administration Server, a connection gateway in a network segment, and a client device (traffic)

| Device | Port number | Name of the process that opens the port | Protocol | Port purpose |
|---|---|---|---|---|
| Administration Server | 13000 | klserver | TCP (TLS) | Receiving connections from Network Agents |
| Network Agent | 13000 | klnagent | TCP (TLS) | Receiving connections from Network Agents |

# Administration Server and two devices in DMZ: a connection gateway and a client device



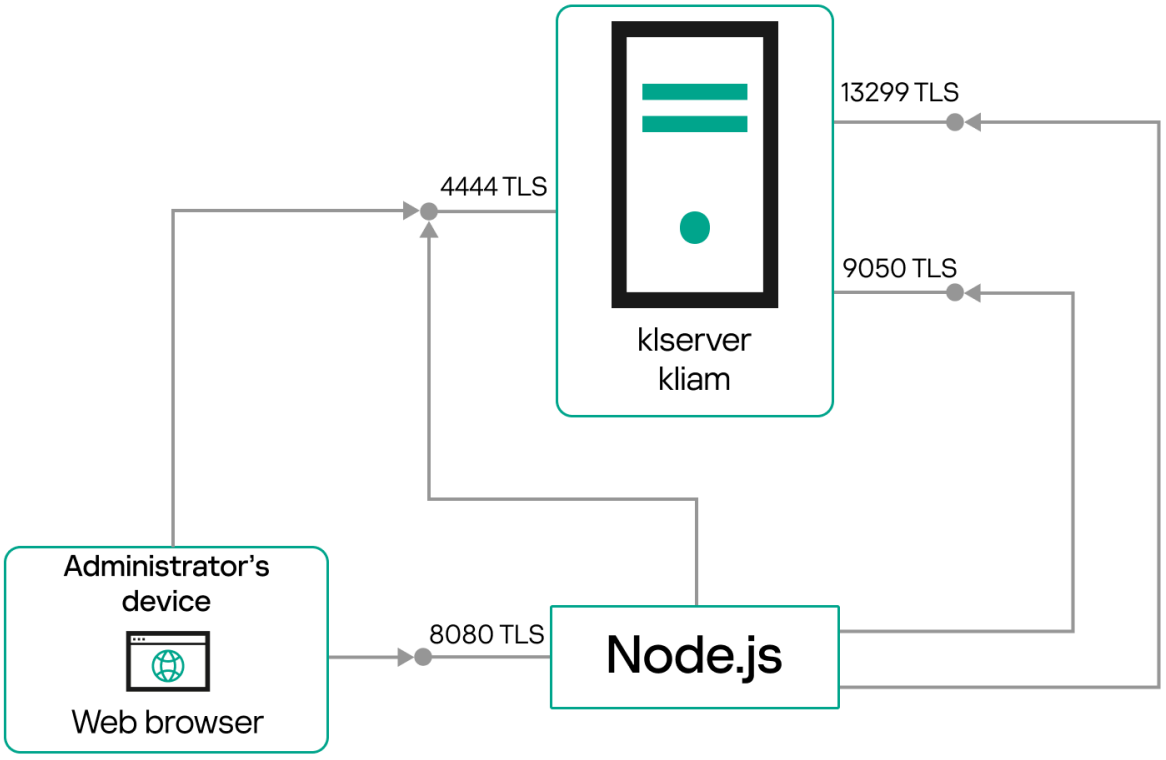

Administration Server with a connection gateway and a client device in DMZ

For schema clarifications, see the table below.

Administration Server, a connection gateway in a network segment, and a client device (traffic)

| Device | Port number | Name of the process that opens the port | Protocol | Port purpose |
|---|---|---|---|---|
| Network Agent | 13000 | klnagent | TCP (TLS) | Receiving connections from Network Agents |

# Administration Server and Kaspersky Security Center Web Console




Administration Server and Kaspersky Security Center Web Console

For schema clarifications, see the table below.

Administration Server and Kaspersky Security Center Web Console (traffic)

| Device | Port number | Name of the process that opens the port | Protocol | Port purpose |
|---|---|---|---|---|
| Administration Server | 13299 | klserver | TCP (TLS) | Receiving connections from Kaspersky Security Center Web Console and Identity and Access Manager (IAM) to the Administration Server over OpenAPI |
| Kaspersky Security Center Web Console Server or Administration Server | 8080 | Node.js: Server-side JavaScript | TCP (TLS) | Receiving connections from Kaspersky Security Center Web Console |
| Administration Server | 4444 | kliam | TCP (TLS) | Receiving connections from Kaspersky Security Center Web Console Server and the browser (used with Kaspersky Security Center Web Console) to Administration Server with IAM over the OpenID Connect authentication protocol |
| Administration Server | 9050 | kliam | TCP (TLS) | Receiving connections from Kaspersky Security Center Web Console to IAM |

Kaspersky Security Center Web Console can be installed on the Administration Server or on another device.

# Quick start guide

Following this scenario, you can install Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console, perform initial setup of the Administration Server by using the quick start wizard, and install Kaspersky applications on managed devices by using the Protection deployment wizard.

## Prerequisites

You must have a license key (activation code) for Kaspersky Endpoint Security for Business or license keys (activation codes) for Kaspersky security applications.

If you first want to try out Kaspersky Security Center Linux, you can get a free 30-day trial at the Kaspersky website.

## Stages

The main installation scenario proceeds in stages:

### 1 Selecting a structure for protection of an enterprise

Find out more about the Kaspersky Security Center Linux components. Based on the network configuration and throughput of communication channels, define the number of Administration Servers to use and how they must be distributed among your offices (if you run a distributed network). Follow the recommendations for choosing the structure of the network.

Define whether a hierarchy of Administration Servers will be used in your organization. To do this, you must evaluate whether it is possible and expedient to cover all client devices with a single Administration Server or it is necessary to build a hierarchy of Administration Servers.

### 2 Preparation for the use of custom certificates

If your organization's Public Key Infrastructure (PKI) requires that you use custom certificates issued by a specific certification authority (CA), prepare those certificates and make sure that they meet all the requirements.

### 3 Configuring network access

Set up interaction of components on your organization's network in accordance with the protection structure chosen at step 1.

To do this, you must:

- Open network access as necessary.
- Ensure the ability to connect to Kaspersky servers or establish an update workflow with a different update source.
- For connection of managed devices to the Administration Server from the internet, configure access via connection gateways or place the Administration Server in the DMZ.

## 4 Sizing the equipment and planning the installation of components

If you intend to install all components of Kaspersky Security Center Linux on the same server, use ready-made sizing calculations from the settings file of the quick installation script (klfi_netsize). Make sure that all the requirements for using the automated component deployment script are a good fit for your infrastructure.

Otherwise, perform a full hardware sizing calculation for the Administration Server, DBMS and Web Console, taking into account the hardware and software requirements and the section on calculating hardware resources for deploying the solution manually, component by component.

To increase the level of protection of Kaspersky Security Center Linux, make sure to include the hardware requirements of the Kaspersky Endpoint Security for Linux application in your calculations.

## 5 Installing Kaspersky Security Center Linux components

Install an operating system supported by the Administration Server and Kaspersky Security Center Web Console on the target devices on which you want to deploy the solution.

Install Kaspersky Security Center Linux in accordance with the planned deployment type:

- Using the automated quick installation script.
- Following the instructions for manual installation and configuration of the Administration Server and Web Console components.

## 6 Installing Kaspersky Endpoint Security for Linux and Network Agent on the Administration Server device

By default, the application does not consider the Administration Server device as a managed device. To protect Administration Server and manage this device, install Kaspersky Endpoint Security for Linux and Network Agent for Linux on the Administration Server device. In this case, Network Agent for Linux is installed and works independently from the server version of Network Agent that you installed together with Administration Server.

Manage the required security settings for Kaspersky Security Center Linux in accordance with the recommendations in the Kaspersky Endpoint Security for Linux Help.

For details, see the "Configuring Anti-Virus protection of the Administration Server" step in the section with the scenario for migration to Kaspersky Security Center Linux using the quick installation script.

## 7 Performing initial setup

When you connect to the Administration Server via the Web Console for the first time, the quick start wizard starts automatically.

During the initial configuration stage, the wizard uses the default settings to create the policies and tasks that are required for protection deployment. However, the default settings may be less than optimal for the needs of your organization. If necessary, you can edit the settings of policies and tasks.

## 8 Discovery of networked devices

Configure and poll the network to discover the devices manually. Kaspersky Security Center Linux receives the addresses and names of all devices detected on the network. You can then use Kaspersky Security Center Linux to install Kaspersky applications and software from other vendors on the detected devices. Kaspersky Security Center Linux regularly starts device discovery, which means that if any new instances appear on the network, they will be detected automatically.

## 9 Arranging devices into administration groups

In some cases, deploying protection on networked devices in the most convenient way may require you to divide the entire pool of devices into administration groups taking into account the structure of the organization. You can create moving rules to distribute devices among groups or you can distribute devices manually. You can assign group tasks for administration groups, define the scope of policies, and assign distribution points.

Make sure that all managed devices have been correctly assigned to the appropriate administration groups, and that there are no longer any unassigned devices in the network.

## 10 Assigning distribution points

We recommend that you use distribution points on large-scale networks to reduce the load on the Administration Server, and on networks that have a distributed structure to provide the Administration Server with access to devices (or device groups) communicated through channels with low throughput rates. Distribution points for administration groups can be assigned automatically or manually.

You can assign connection gateways only when assigning distribution points manually.

To do this:

- Make sure you have enough distribution points after switching the assignment mode to manual.
- Configure the necessary connections of the Administration Server and connection gateways before proceeding with the deployment of Network Agents on devices of network locations in which the devices must connect to the Administration Server through a connection gateway.

### 11 Installing Network Agent and security applications on networked devices

Deployment of protection on an enterprise network entails installation of Network Agent and security applications on devices that have been detected by Administration Server during the device discovery.

To install the applications remotely, run the Protection deployment wizard.

Security applications protect devices against viruses and other programs that pose a threat. Network Agent ensures communication between the device and Administration Server. Network Agent settings are configured automatically by default.

Before you start installing Network Agent and the security applications on networked devices, make sure that these devices are accessible (turned on).

### 12 Deploying license keys to client devices

Deploy license keys to client devices to activate managed security applications on those devices.

### 13 Configuring Kaspersky application policies

To apply different application settings to different devices, you can use device-centric security management and/or user-centric security management. Device-centric security management can be implemented by using policies and tasks. You can apply tasks only to those devices that meet specific conditions. To set the conditions for filtering devices, use device selections and tags.

### 14 Monitoring the network protection status

You can monitor your network by using widgets on the dashboard, generate reports from Kaspersky applications, configure and view selections of events received from the applications on the managed devices, and view notification lists.

Long-term storage of events, prompt receipt of events, processing and correlation must be performed in an external system specializing on SIEM tasks.

Indicators of the solution components are tracked using the SNMP protocol in IT infrastructure monitoring systems and other third-party agent solutions.

Continuous monitoring of the protection status is available in the Web Console in the **Hardening center** section.

# Hardening Guide

Kaspersky Security Center Linux is designed for centralized execution of basic administration and maintenance tasks on an organization's network. The application provides the administrator access to detailed information about the organization's network security level. Kaspersky Security Center Linux allows you to configure all components of protection built by using Kaspersky applications.

Kaspersky Security Center Linux Administration Server has full access to protection management of client devices and is the most important component of the organization's security system. Therefore, increased protection methods are required for Administration Server.

Before configuring, create a Kaspersky Security Center Linux Administration Server backup copy by using the Backup of Administration Server data task or the klbackup utility. Keep the backup copy of the data in a safe place.

The Hardening Guide describes recommendations and features of configuring Kaspersky Security Center Linux and its components, aimed to reduce the risks of its compromise.

The Hardening Guide contains the following information:

- Selecting the Administration Server architecture
- Configuring a secure connection to Administration Server
- Configuring accounts to access Administration Server
- Managing protection of Administration Server
- Managing protection of client devices
- Configuring protection for managed applications
- Administration Server maintenance
- Transferring information to third-party applications
- Security recommendations for third-party information systems

# Hardening checklist

Administration Server deployment

- Install Administration Server on a dedicated physical or virtual server.
- Do not use the dedicated server for running other services.
- Do not install Administration Server (hereinafter referred to as the Server) on a:
  - Domain controller
  - Terminal server
  - User device

### Connection safety

- Configure a firewall to restrict access to the Server device on all ports and protocols except for the ports required by the Server. Allow access to the Server device only from trusted devices.
- Configure an allowlist of IP addresses for Server ports used to connect Kaspersky Security Center Web Console (also referred to as Web Console) to Server.
- Configure the firewall to allow access to Server through Web Console only from trusted devices.
- Configure the TLS protocol version 1.2 or higher on Server.
- Configure a firewall to restrict access to the device with the Server DBMS installed.
- Configure SSL authentication between Server and DBMS (MySQL or PostgreSQL).

### Accounts and authentication

- Configure two-factor authentication (TOTP, RFC 6238) for Server access.
- Do not install the authenticator application on the same device from which the connection to Server through Web Console is established.
- Use multi-factor authentication (MFA) for access to the Server device by using a token, a smart card, or other method.
- Create a dedicated administration group for the Server device and create a special security policy for it.
- Restrict the number of users who have the Main Administrator role.
- Configure access rights to Server features based on roles of users and groups.
- Allow remote installation of applications only for a separate user account.
- Conduct a regular audit of all users on the Server device.

### Managing protection of Administration Server

- Install a security application on the Server device:
  - For a physical server – Kaspersky Endpoint Security
  - For a virtual server – Kaspersky Security for Virtualization
- Create and apply a separate policy for Server protection (different from the security policies for other managed devices).

- Create and apply a separate password for Server protection (different from the password for other managed devices).
- Enable all available protection modules in the security application (for information about the security settings required for using the Administration Server, refer to the Kaspersky Endpoint Security for Linux Help).

Configuring policies and tasks for managed applications

- Create and apply policies to all managed devices or to the group with new managed devices for the following applications:
  - Network Agent
  - Kaspersky Endpoint Security for Windows/Linux/macOS
  - Kaspersky Endpoint Agent (or other Kaspersky applications)
- Enable password protection against disabling protection or uninstalling Kaspersky applications.
- Lock policy settings (close the "lock") to prevent the reassignment of these settings on managed devices.
- Create a scheduled full scan task of all devices.
- Enable the use of Kaspersky Security Network (KSN) and accept the latest KSN Statement.
- Configure device discovery and specify the default administration group for newly discovered devices.
- Restrict the use of automatic rules for moving devices between administration groups.
- Protect distribution points from unauthorized access.
- Avoid assigning distribution points automatically in small networks or high-importance networks.

Administration Server maintenance

- Do not delete or disable the following tasks:
  - Backup
  - Administration Server maintenance
- Regularly install OS and third-party software updates.

### Event transfer to third-party systems

- Configure monitoring and reporting of security events.
- Configure event export to a SIEM system.
- Configure Server notifications for:
  - Audit events
  - Critical events
  - Failure events and warnings

### Security recommendations for third-party information systems

- Apply CIS Benchmarks security recommendations to the used operating systems, DBMS, and hypervisors.
- For Astra Linux, follow the security recommendations from the corresponding Red Book version.
- For RED OS, follow the recommendations provided in the official RED OS documentation.

## Administration Server deployment

### Administration Server architecture

In general, the choice of a centralized management architecture depends on the location of protected devices, access from adjacent networks, delivery schemes of database updates, and so on.

At the initial stage of architecture development, we recommend getting acquainted with the Kaspersky Security Center Linux components and their interaction with each other, as well as with schemas for data traffic and port usage.

Based on this information, you can form an architecture that specifies:

- The Administration Server location and network connections
- Organization of the administrator's workspaces, and methods of connecting to Administration Server
- Deployment methods for Network Agent and protection software
- Using distribution points
- Using virtual Administration Servers
- Using a hierarchy of Administration Servers

- Anti-virus database update scheme
- Other information flows

### Selecting a device for the Administration Server installation

We recommend that you install Administration Server on a dedicated server in the organization infrastructure. If there is no other third-party software installed on the server, you can configure the security settings based on the requirements of Kaspersky Security Center Linux, without depending on the requirements of third-party software.

You can deploy Administration Server on a physical server or on a virtual server. Please make sure that the selected device meets the hardware and software requirements.

### Restriction of deploying Administration Server on a domain controller, a terminal server, or a user device

We strongly do not recommend installing Administration Server on a domain controller, a terminal server, or a user device.

We recommend that you provide functional separation of the network key nodes. This approach allows you to maintain the operability of different systems when a node fails or is compromised. At the same time, you can create different security policies for each node.

### Accounts for installing and running Administration Server

During the deployment of Administration Server, it is necessary to create two unprivileged accounts. The services that are included in Administration Server will work under these unprivileged accounts. Follow the principle of least privilege when you grant rights and permissions to the accounts. Avoid including unnecessary accounts in the 'kladmins' group.

You also need to create an internal DBMS account. Administration Server uses this internal DBMS account to access the selected DBMS.

The set of required accounts and their rights depends on the selected DBMS type and the method of the Administration Server database creation.

## Connection safety

### Usage of TLS

We recommend prohibiting insecure connections to Administration Server. For example, you can prohibit connections that use HTTP in the Administration Server settings.

Please note that by default, several HTTP ports of Administration Server are closed. The remaining port is used for the Administration Server Web Server (8060). This port can be limited by the firewall settings of the Administration Server device.

### Strict TLS settings

We recommend using TLS protocol version 1.2 and later, and restricting or prohibiting insecure encryption algorithms.

You can configure the encryption protocols (TLS) used by Administration Server. Please note that at the time of the release of a version of Administration Server, by default the encryption protocol settings are configured to ensure secure data transfer.

### Restricting access to the Administration Server database

We recommend restricting access to the Administration Server database. For example, grant access only from the Administration Server device. This reduces the likelihood of the Administration Server database being compromised due to known vulnerabilities.

You can configure the parameters according to the operating instructions of the used database, as well as provide closed ports on firewalls.

### Security interaction with an external DBMS

If the DBMS is installed on a separate device during the installation of Administration Server (external DBMS), we recommend configuring the parameters for secure interaction and authentication with this DBMS. For more information on configuring SSL authentication, see Authenticating PostgreSQL Server and Scenario: Authenticating MySQL Server.

### Configuring an allowlist of IP addresses to connect to Administration Server

By default, Kaspersky Security Center Linux users can log in to Kaspersky Security Center Linux from any device where Kaspersky Security Center Web Console or OpenAPI applications are installed. You can configure Administration Server so that users can connect to it only from devices with allowed IP addresses. For example, if an intruder tries to connect to Kaspersky Security Center Linux through Kaspersky Security Center Web Console Server installed on a device that is not included in the allowlist, he or she will not be able to log in to Kaspersky Security Center Linux.

### Configuring an allowlist of IP addresses to connect to Kaspersky Security Center Web Console

By default, Kaspersky Security Center Linux users can connect to Kaspersky Security Center Web Console from any device. On a device with Kaspersky Security Center Web Console, you must configure the firewall (built into the operating system or a third-party one) so that users can connect to Kaspersky Security Center Web Console only from allowed IP addresses.

### Security of connection to the domain controller during the polling

To poll the domain controller, Administration Server or a Linux distribution point tries to connect to this domain over LDAPS. By default, certificate verification is not required when connecting. To enforce certificate verification, set the `KLNAG_LDAP_TLS_REQCERT` flag to 1. Also, you can specify a custom path to the certificate authority (CA) to access the certificate chain by using the `KLNAG_LDAP_SSL_CACERT` flag.

## Accounts and authentication

Before following these steps, create a backup copy of Kaspersky Security Center Linux Administration Server data using the Backup of Administration Server data task or the klbackup utility and save the backup copy in a safe location. Keep the backup copy of the data in a safe place.

### Using two-factor authentication with Administration Server

**Kaspersky Security Center Linux uses two-factor authentication** when signing in to Kaspersky Security Center Web Console, based on the RFC 6238 standard (TOTP: Time-Based One-Time Password algorithm).

Every time you log in to Kaspersky Security Center Web Console, you enter your user name, password, and an additional one-time security code. To receive a one-time security code, you must install an authenticator app on your computer or your mobile device.

There are both software and hardware authenticators (tokens) that support the RFC 6238 standard. Examples of software authenticators include Kaspersky Password Manager for Business, Google Authenticator, Microsoft Authenticator, FreeOTP.

We strongly do not recommend installing the authenticator app on the same device from which the connection to Administration Server is established. You can install an authenticator app on your mobile device.

### Using two-factor authentication for an operating system

To ensure comprehensive protection by using two-factor authentication, it is necessary to secure not only Administration Server but also the device on which it is installed.

When connecting to the device where Administration Server is installed (via SSH, RDP, or other protocols), we recommend using multi-factor authentication (MFA) with a token, smart card, or another authentication method.

### Prohibition on saving the administrator password

If you use Kaspersky Security Center Web Console, we do not recommend saving the administrator password in the browser installed on the user device.

### Authentication of an internal user account

By default, the password of an internal user account of Administration Server must comply with the following rules:

- The password must be 8 to 256 characters long.
- The password must contain characters from at least three of the groups listed below:
  - Uppercase letters (A–Z)
  - Lowercase letters (a-z)
  - Numbers (0–9)
  - Special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- The password must not contain any whitespaces, Unicode characters, or the combination of "." and "@", when "." is placed before "@".

By default, the maximum number of allowed password entry attempts is 10. You can change the number of allowed password entry attempts.

The Kaspersky Security Center Linux user can enter an invalid password a limited number of times. After the limit is reached, the user account is blocked for one hour.

### Configuring the options for changing the password of an internal user account

We recommend configuring the following options for changing the password of an internal user account:

- Password rotation period
- Time of the preliminary warning about the need to change the password
- Value of the **User must change password at first sign-in** option

### Account protection from unauthorized modification

We recommend enabling an additional option to protect an internal user account of Administration Server from unauthorized modification. This protection must be configured separately for each internal user.

### Dedicated administration group for Administration Server

For Administration Server

We recommend creating a dedicated administration group. Grant this group special access rights and create a special security policy for it.

To avoid intentionally lowering the security level of Administration Server, we recommend restricting the list of accounts that can manage the dedicated administration group.

### Restricting the assignment of the Main administrator role

The user created by the kladduser utility is assigned the Main Administrator role in the access control list (ACL) of Administration Server or virtual Administration Server. We recommend avoiding the assignment of the Main Administrator role to a large number of users.

### Configuring access rights to application features

We recommend using flexible configuration of access rights to the features of Kaspersky Security Center Linux for each user or group of users.

Role-based access control allows the creation of standard user roles with a predefined set of rights and the assignment of those roles to users depending on their scope of duties.

The main advantages of the role-based access control model:

- Ease of administration
- Role hierarchy
- Least privilege approach
- Segregation of duties

You can assign built-in roles to certain employees based on their positions, or create completely new roles.

While configuring roles, pay attention to the privileges associated with changing the protection state of Administration Server device and remote installation of third-party software:

- Managing administration groups
- Operations with Administration Server
- Remote installation
- Changing the parameters for storing events and sending notifications.

  This privilege allows you to set notifications that run a script or an executable module on the Administration Server device when an event occurs.

### Separate account for remote installation of applications

In addition to the basic differentiation of access rights, we recommend restricting the remote installation of applications for all accounts (except for the Main administrator or another specialized account).

We recommend using a separate account for remote installation of applications. You can assign a role or permissions to the separate account.

### Regular audit of all users and users' actions

We recommend conducting a regular audit of all users on the Administration Server device. This allows you to respond to certain types of security threats associated with the possible compromise of a device.

Also, you can track the users' actions, such as connecting to and disconnecting from Administration Server, connecting to Administration Server with an error, and objects modification (for objects that support revision management).

# Managing protection of Administration Server

### Selecting an Administration Server protection software

Depending on the type of the Administration Server deployment and the general protection strategy, select the application to protect the Administration Server device.

If you deploy Administration Server on a dedicated device, we recommend selecting the Kaspersky Endpoint Security application to protect the Administration Server device. This allows applying all available technologies to protect the Administration Server device, including behavioral analysis modules.

If Administration Server is installed on a device that exists in the infrastructure and has previously been used for other tasks, we recommend considering the following protection software:

- Kaspersky Industrial CyberSecurity for Nodes. We recommend installing this application on devices that are included in an industrial network. Kaspersky Industrial CyberSecurity for Nodes is an application that has certificates of compatibility with various manufacturers of industrial software.

- Recommended security applications. If Administration Server is installed on a device with other software, we recommend taking into account the recommendations from that software vendor on the compatibility of security products (there may already be recommendations for selecting a security solution, and you may need to configure the trusted zone).

### Creating a separate security policy for the protection application

We recommend that you create a separate security policy for the application that protects the Administration Server device. This policy must be different from the security policy for client devices. This allows specifying the most appropriate security settings for Administration Server, without affecting the protection level of other devices.

We recommend dividing devices into groups, and then placing the Administration Server device into a separate group for which you can create a special security policy.

### Protection modules

If there are no special recommendations from the vendor of the third-party software installed on the same device as Administration Server, we recommend activating and configuring all available protection modules (after checking the operation of these protection modules for a certain time).

### Configuring the firewall of the Administration Server device

On the Administration Server device, we recommend configuring the firewall to restrict the number of devices from which administrators can connect to Administration Server through Kaspersky Security Center Web Console.

By default, Administration Server uses port 13299 to receive connections from Kaspersky Security Center Web Console. We recommend restricting the number of devices from which Administration Server can be managed by using this port.

## Managing protection of Network Agent

To prevent attackers from taking devices out of control of your Administration Server, we strongly recommend described these practices:

### Using the uninstall password

In the settings of the Network Agent installation package, specify the uninstallation password that will be requested when uninstalling Network Agent.

Functionality is available only for Network Agent on devices running Windows operating systems.

### Hardening the Network Agent

In the settings of the Network Agent installation package, enable the **Protect Network Agent service against unauthorized removal or termination, and prevent changes to the settings** option. After Network Agent is installed on a managed device, the component cannot be uninstalled or modified without required privileges. The Network Agent service cannot be stopped.

Functionality is available only for Network Agent on devices running Windows operating systems.

### Keeping track of the Administration Server address to which the Network Agent connects

To catch any unauthorized switching of Network Agent to an outside Administration Server, use the Kaspersky Event Log. Kaspersky Event Log is a section of the event log that is stored in the operating system on managed devices. On Windows, you can view the contents of the log using the Event Viewer, and on Linux, using the journalctl utility.

When Network Agent connects to the Administration Server, one or two entries are written to the Kaspersky Event Log with the following information:

- Administration Server address:
  - **Try to connect to Administration Server at <Administration Server address>**.
  - **Connected to Administration Server at <Administration Server address>**.
- The address of the Administration Server and the connection gateway when connecting through a gateway:
  - **Try to connect to Administration Server at <Administration Server address> via CG <connection gateway address>**.
  - **Connected to Administration Server at <Administration Server address> via CG <connection gateway address>**.

An event with the address of the Administration Server is registered in the following cases:

- Every time the Network Agent service is restarted
- When Network Agent connects to another Administration Server
- Once a day during normal operation of the device, even if the Network Agent service has not been restarted and the Network Agent has not connected to another Administration Server (in this case, only the first entry is republished to the log)

For convenience, we recommend configuring the upload of events from the Kaspersky Event Log to a SIEM system and generating an alert if the Administration Server address indicated in the event does not match the current address of your Administration Server.

*To configure the upload of events from the Kaspersky Event Log:*

1. In the SIEM system, configure the receipt of events from Kaspersky Event Log from all managed devices.
2. Create a correlation rule that is triggered when an event about the change of the Administration Server to which the Network Agent is connected is received.
3. Configure the creation of an alert when this correlation rule is triggered.
4. If necessary, configure the sending of alert notifications by email or create a widget with information about alerts on the dashboard.

# Managing protection of client devices

## Restricting of adding license keys to installation packages

Installation packages are stored in the Administration Server shared folder, in the Packages subfolder. If you add a license key to an installation package, the license key can be accessed by all users with read rights to this folder (directly or via the Web server embedded in Administration Server).

To avoid compromising the license key, we do not recommend adding license keys to installation packages.

We recommend using automatic distribution of license keys to managed devices, deployment through the Add license key task for a managed application, and adding an activation code or a key file manually to the devices.

## Automatic rules for moving devices between administration groups

We recommend restricting the use of automatic rules for moving devices between administration groups.

If you use automatic rules for moving devices, this may lead to propagation of policies that provide more privileges to the moved device than the device has before relocation.

Also, moving a client device to another administration group may lead to propagation of policy settings. These policy settings may be undesirable for distribution to guest and untrusted devices.

This recommendation does not apply for one-time initial allocation of devices to administration groups.

## Security requirements for distribution points and connection gateways

Devices with Network Agent installed can act as a distribution point and perform the following functions:

- Distribute updates and installation packages received from Administration Server to client devices within the group.
- Perform remote installation of third-party software and Kaspersky applications on client devices.
- Poll the network to detect new devices and update information about existing ones. A distribution point can apply the same device discovery methods as the Administration Server.

Placing distribution points on the organization's network used for:

- Reducing the load on Administration Server
- Traffic optimization
- Providing Administration Server with access to devices in hard-to-reach parts of the network

Taking into account the available capabilities, we recommend protecting devices that act as distribution points from any type of unauthorized access (including physically).

## Restricting automatic assignment of distribution points

To simplify administration and keep the network operability, we recommend using automatic assignment of distribution points. However, for industrial networks and small networks, we recommend that you avoid assigning distribution points automatically, since, for example, the private information of the accounts used for pushing remote installation tasks, can be transferred to distribution points by means of the operating system.

For industrial networks and small networks, you can manually assign devices to act as distribution points.

You can also view the Report on activity of distribution points.

## Security requirements for devices of Kaspersky Security Center Linux users

Special security requirements must be applied to Kaspersky Security Center Linux users' devices. We recommend protecting these devices against any type of unauthorized access (including physically).

Kaspersky Security Center Linux user devices include the following:

- Devices from which Kaspersky Security Center Linux users connect to Kaspersky Security Center Web Console by using a browser.
- Devices from which applications that interact with Administration Server via OpenAPI are connected to Kaspersky Security Center Linux.

### Security requirements for devices with Kaspersky Security Center Web Console installed

Devices with Kaspersky Security Center Web Console installed are used to manage Kaspersky Security Center Linux, so special requirements must apply to the security of these devices. We recommend protecting these devices against any type of unauthorized access (including physically).

## Configuring protection for managed applications

### Managed application policies

We recommend creating a policy for each type of used applications and components of Kaspersky Security Center Linux (Network Agent, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Agent, and others). This policy must be applied to all managed devices (the root administration group) or to a separate group to which new managed devices are automatically moved according to the configured movement rules.

### Specifying the password for disabling protection and uninstalling the application

**We strongly recommend enabling password protection to prevent intruders from disabling or uninstalling Kaspersky security applications.** On platforms where password protection is supported, you can set the password, for example, for Kaspersky Endpoint Security, Network Agent, and other Kaspersky applications. After you enable password protection, we recommend locking the corresponding settings by closing the "lock."

### Specifying the password for manual connection of a client device to the Administration Server (klmover utility)

The klmover utility allows you to manually connect a client device to the Administration Server. The klmover utility is located in the Network Agent installation folder.

To prevent intruders from moving devices out of your Administration Server's control, we strongly recommend enabling password protection for running the klmover utility. To enable password protection, select the **Use uninstallation password** option in the Network Agent policy settings.

The klmover utility requires local administrator rights.

If you lose or forget the password from the password-protected Network Agent installed on the device that is no longer under the management of Kaspersky Security Center Linux, you cannot remove Network Agent by using the klmover utility or the command line. In this case, you have to reinstall the operating system on the device with the installed password-protected Network Agent.

Enabling the **Use uninstallation password** option on Windows devices also enables password protection for the Cleaner tool (cleaner.exe).

### Using Kaspersky Security Network

In all policies of managed applications and in the Administration Server properties, we recommend enabling the use of Kaspersky Security Network (KSN) and accepting the KSN Statement. When you update or upgrade Administration Server, you can accept the updated KSN Statement. In some cases, when the use of cloud services is prohibited by law or other regulations, you can disable KSN.

### Regular scan of managed devices

For all device groups, we recommend creating a task that periodically runs a full scan of devices.

### Discovering new devices

We recommend properly configuring device discovery settings: set up integration with domain controllers and specify IP address ranges for discovering new devices.

For security purposes, you can use the default administration group that includes all new devices and the default policies affecting this group.

## Administration Server maintenance

### Backup copying of Administration Server data

Data backup allows you to restore Administration Server data without data loss.

By default, a data backup task is created automatically after the installation of Administration Server and is executed periodically, saving backups in the appropriate directory.

Settings of the data backup task can be changed as follows:

- The backup frequency increases
- A special directory for saving copies is specified
- Passwords for backup copies is changed

If you store backup copies in a special directory, that is different from the default directory, we recommend limiting the access control list (ACL) for this directory. The Administration Server accounts and accounts of the Administration Server database must have the write access for this directory.

### Administration Server maintenance

The Administration Server maintenance allows you to reduce the database volume, and improve the performance and operation reliability of the application. We recommend that you maintain Administration Server at least every week.

The Administration Server maintenance is performed using the dedicated task. The application performs the following actions when maintaining the Administration Server:

- Re-organizes database indexes
- Updates the database statistics
- Shrinks the database (if necessary)

### Installing operating system updates and third-party software updates

We strongly recommend that you regularly install software updates for the operating system and third-party software on the Administration Server device.

Client devices do not require a continuous connection to Administration Server, so it is safe to reboot the Administration Server device after installing updates. All events registered on client devices during Administration Server downtime are sent to it after the connection is restored.

## Event transfer to third-party systems

### Monitoring and reporting

For timely response to security issues, we recommend configuring the monitoring and reporting features.

### Export of events to SIEM systems

For fast detection of security issues before significant damage occurs, we recommend using event export in a SIEM system.

### Email notifications of audit events

Kaspersky Security Center Linux allows you to receive information about events that occur during the operation of Administration Server and Kaspersky applications installed on managed devices. For timely response to emergencies, we recommend configuring Administration Server to send notifications about the audit events, critical events, failure events, and warnings that it publishes.

Since these events are intra-system events, a small number of them can be expected, which is quite applicable for mailing.

## Security recommendations for third-party information systems

### Security recommendations from CIS Benchmarks

When using versions of operating systems, virtualization platforms, or database servers supported by Administration Server and Network Agent, we recommend applying the best information security practices from the Center for Internet Security (CIS), if any, to fine-tune these information systems.

Center for Internet Security (CIS) is a non-profit organization dedicated to improving security in the field of information technology. In particular, CIS develops and distributes safety standards such as CIS Controls and CIS Benchmarks. These standards are a set of recommendations and practices for ensuring the security of information systems.

The CIS portal contains recommendations for the versions of the following information systems supported by Administration Server and Network Agent:

- Operating systems of the following families:
  - Windows for desktops
  - Windows for servers
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux

- SUSE Linux Enterprise Server
- macOS

- VMware virtualization platforms
- Database servers:
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

### Security recommendations for the Astra Linux operating system

When using the Astra Linux operating system, you should follow the security recommendations described in the Red Book for the corresponding version of Astra Linux.

### Security recommendations for the RED OS operating system

When using the RED OS operating system, you should use the security recommendations from the administrator's guide described in the official RED OS documentation.

## Recommendations for using Kaspersky security applications

### Using the KLAdmin password in Kaspersky Endpoint Security for Windows

The KLAdmin account is an administrator account with unrestricted access to Kaspersky Endpoint Security for Windows. The KLAdmin account has the right to perform any password-protected action in Kaspersky Endpoint Security for Windows, including removing the application. The permissions for the KLAdmin account cannot be revoked. You can set the password for the KLAdmin account in the properties of the Kaspersky Endpoint Security for Windows policy. The Kaspersky Endpoint Security for Windows administrator is fully responsible for the safe use of the password for the KLAdmin account. If your organization has its own password policy, follow the instructions of that policy. The longer and more complex the password, the more reliable it is.

Our recommendations for protecting the organization from theft of the KLAdmin password are as follows:

- **General requirements**

  Do not use the account name or part of the name as the password.

- **Minimum password length requirements**

  Create a password that is at least 10 characters in length.

- **Requirements for using multiple character types**

  Set a complex password that contains characters from different categories: lowercase and uppercase letters, numbers, and special characters.

- **Password expiration requirements**

  Set a minimum password expiration date of 90 days. A new password must not match any of the last 24 passwords.

# Scenario: Authenticating MySQL Server

We recommend that you use a TLS certificate to authenticate the MySQL server. You can use a certificate from a trusted certification authority (CA) or a self-signed certificate.

Administration Server supports both one-way and two-way SSL authentication for MySQL.

## Enable one-way SSL authentication

Follow these steps to configure one-way SSL authentication for MySQL:

1. **Create a self-signed TLS certificate for the MySQL server**

   Execute the following command:

   ```
   openssl genrsa 1024 > ca-key.pem
   ```

   ```
   openssl req -new -x509 -nodes -days 365 -key ca-key.pem -config myssl.cnf > ca-cert.pem
   ```

   ```
   openssl req -newkey rsa:1024 -days 365 -nodes -keyout server-key.pem -config myssl.cnf
   > server-req.pem
   ```

   ```
   openssl x09 -req -in server-req.pem -days 365 -CA ca-cert.pem -CAkey ca-key.pem -
   set_serial 01 > server-cert.pem
   ```

2. **Create a server flag file**

   Use the klscflag utility to create the KLSRV_MYSQL_OPT_SSL_CA server flag and specify the path to the certificate as its value. The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <path to ca-cert.pem> -t d
   ```

3. **Configure the database**

   Specify the certificates in the my.cnf file. Open the my.cnf file in a text editor and add the following lines into the [mysqld] section:

   ```
   [mysqld]
   ```

   ```
   ssl-ca=".../mysqlcerts/ca-cert.pem"
   ```

   ```
   ssl-cert=".../mysqlcerts/server-cert.pem"
   ```

   ```
   ssl-key=".../mysqlcerts/server-key.pem"
   ```

Enable two-way SSL authentication

Follow these steps to configure two-way SSL authentication for MySQL:

1. **Create server flag files**

   Use the klscflag utility to create the server flags and specify the path to the certificate files as their values:

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <path to ca-cert.pem> -t s
   ```

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <path to server-cert.pem> -t s
   ```

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <path to server-key.pem> -t s
   ```

   The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.

2. **Specify the passphrase (optional)**

   If the server-key.pem requires a passphrase, create a KLSRV_MARIADB_OPT_TLS_PASPHRASE flag and specify the passphrase as its value:

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <passphrase> -t s
   ```

3. **Configure the database**

   Specify the certificates in the my.cnf file. Open the my.cnf file in a text editor and add the following lines into the [mysqld] section:

   ```
   [mysqld]
   ```

   ```
   ssl-ca=".../mysqlcerts/ca-cert.pem"
   ```

   ```
   ssl-cert=".../mysqlcerts/server-cert.pem"
   ```

   ```
   ssl-key=".../mysqlcerts/server-key.pem"
   ```

# Scenario: two-way TLS authentication of PostgreSQL for the Administration Server database and the IAM database

In Kaspersky Security Center Linux, you can configure encryption and mutual validation of certificates between the PostgreSQL server and clients, that is, the Administration Server and IAM. Each database uses a separate user and a separate client certificate. In addition to TLS, `scram-sha-256` password authentication is used.

Authenticating PostgreSQL Server proceeds in stages:

1. **Preparing the DBMS and creating roles**

   Run the following commands:

```
sudo -u postgres psql
CREATE DATABASE kav;
CREATE DATABASE iam;
CREATE USER myuserksc WITH PASSWORD '*password*';
ALTER ROLE myuserksc WITH LOGIN CREATEDB;
ALTER DATABASE kav OWNER TO myuserksc;
CREATE USER myuseriam WITH PASSWORD '*password*';
ALTER ROLE myuseriam WITH LOGIN CREATEDB;
ALTER DATABASE iam OWNER TO myuseriam;
```

2. **Creating your own CA and server certificate (one-way SSL authentication)**

   `subjectAltName` (SAN) is a required parameter of the server certificate. The value of this parameter must match the FQDN of the host.

   Run the following commands:

```
sudo openssl req -x509 -nodes -newkey rsa:4096 -keyout /etc/ssl/private/postgresql_ca.key -out
/etc/ssl/certs/postgresql_ca.crt -days 365 -addext "subjectAltName=DNS:*FQDN*" -subj "/CN=mysrvca"
sudo openssl req -new -nodes -newkey rsa:4096 -keyout /etc/ssl/private/postgresql_leaf.key -out
/tmp/postgresql_leaf.csr -addext "subjectAltName=DNS:< FQDN >" -subj "/CN=*FQDN*"
sudo openssl x509 -req -in /tmp/postgresql_leaf.csr -CA /etc/ssl/certs/postgresql_ca.crt -CAkey
/etc/ssl/private/postgresql_ca.key -CAcreateserial -out /etc/ssl/certs/postgresql_leaf.crt -days 365 -sha256 -
copy_extensions copy
sudo cat /etc/ssl/certs/postgresql_leaf.crt /etc/ssl/certs/postgresql_ca.crt | sudo tee
/etc/ssl/certs/postgresql.crt
sudo chmod 600 /etc/ssl/private/postgresql_leaf.key
sudo chown postgres:postgres /etc/ssl/private/postgresql_leaf.key
sudo chmod 644 /etc/ssl/certs/postgresql_leaf.crt
sudo chown ksc:kladmins /etc/ssl/certs/postgresql_ca.crt
sudo chmod 644 /etc/ssl/certs/postgresql_ca.crt
sudo chmod 644 /etc/ssl/certs/postgresql.crt
```

3. **Creating client CA and certificates for the Administration Server database and the IAM database (two-way SSL authentication)**

   Run the following commands:

```
sudo openssl req -x509 -nodes -newkey rsa:4096 -keyout /etc/ssl/private/postgresql_cli_ca.key -out
/etc/ssl/certs/postgresql_cli_ca.crt -days 365 -subj "/CN=myclica"
openssl x509 -in /etc/ssl/certs/postgresql_cli_ca.crt -text -noout
sudo chmod 600 /etc/ssl/private/postgresql_cli_ca.key
sudo chmod 644 /etc/ssl/certs/postgresql_cli_ca.crt
openssl req -new -nodes -newkey rsa:4096 -keyout $HOME/postgresql_cli_myuserksc.key -out
/tmp/postgresql_cli_myuserksc.csr -subj "/CN=myuserksc"
sudo openssl x509 -req -in /tmp/postgresql_cli_myuserksc.csr -CA /etc/ssl/certs/postgresql_cli_ca.crt -CAkey
/etc/ssl/private/postgresql_cli_ca.key -CAcreateserial -out $HOME/postgresql_cli_myuserksc.crt -days 365
openssl req -new -nodes -newkey rsa:4096 -keyout $HOME/postgresql_cli_myuseriam.key -out
/tmp/postgresql_cli_myuseriam.csr -subj "/CN=myuseriam"
sudo openssl x509 -req -in /tmp/postgresql_cli_myuseriam.csr -CA /etc/ssl/certs/postgresql_cli_ca.crt -CAkey
/etc/ssl/private/postgresql_cli_ca.key -CAcreateserial -out $HOME/postgresql_cli_myuseriam.crt -days 365
```

### 4 Copying client certificates to the Administration Server and IAM host and setting permissions

Run the following commands:

```
sudo cp $HOME/postgresql_cli_myuserksc.crt   /home/ksc/
sudo cp $HOME/postgresql_cli_myuserksc.key   /home/ksc/
sudo cp $HOME/postgresql_cli_myuseriam.crt   /home/ksciam/
sudo cp $HOME/postgresql_cli_myuseriam.key   /home/ksciam/
sudo chown ksc:kladmins /home/ksc/*.crt /home/ksc/*.key
sudo chown ksciam:kladmins /home/ksciam/*.crt /home/ksciam/*.key
sudo chmod 644 /home/ksc/*.crt
sudo chmod 600 /home/ksc/*.key
sudo chmod 644 /home/ksciam/*.crt
sudo chmod 600 /home/ksciam/*.key
```

### 5 Configuring PostgreSQL

Edit the postgresql.conf file as follows:

```
listen_addresses = '*'
ssl = on
ssl_cert_file = '*path to postgresql.crt*'
ssl_key_file = '*path to postgresql_leaf.key*'
ssl_ca_file = '*path to postgresql_cli_ca.crt*'
```

Modify pg_hba.conf file as follows:

```
hostssl    kav    myuserksc    *Administration Server IP address*    scram-sha-256    clientcert=verify-full
hostssl    iam    myuseriam    *Administration Server IP address*    scram-sha-256    clientcert=verify-full
```

If the Administration Server and PostgreSQL are on the same device, use the `127.0.0.1/32` address and `listen_addresses = 'localhost'`.

Ensure that pg_hba.conf doesn't include a record that starts with `host`.

### 6 Restarting the PostgreSQL daemon

Execute the following command:

```
systemctl restart postgresql
```

### 7 Specifying the server flag for the Administration Server

Use the klscflag utility to create the server flags and specify the path to the certificate files as their values.

The klscflag utility is located in the folder where Administration Server is installed. The default installation path is `/opt/kaspersky/ksc64/sbin/`.

Run the following commands:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v *path to postgresql_cli_myuserksc.crt* -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v *path to postgresql_cli_myuserksc.key* -t s
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v *path to postgresql_ca.crt* -t s
```

If postgres_leaf.key requires a passphrase, create a `KLSRV_POSTGRES_OPT_TLS_PASPHRASE` flag and specify the passphrase as its value:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v *pasphrase* -t s
```

8. **Configuring IAM**

   Edit the iam_config.yaml file as follows:

   ```
   dbms_tl_opt_ssl_ca: "/etc/ssl/certs/postgresql_ca.crt"
   dbms_tl_opt_ssl_verify_server_cn: "1"
   dbms_tl_opt_ssl_cert: "/home/ksc/postgresql_cli_myuseriam.crt"
   dbms_tl_opt_ssl_key:  "/home/ksc/postgresql_cli_myuseriam.key"
   ```

9. **Restarting Administration Server services**

   Execute the following command:

   ```
   sudo systemctl restart kl*
   ```

# Preparation for deployment

This section describes how to choose the option of the Kaspersky Security Center Linux deployment, Kaspersky Security Center Linux configuration, and a DBMS according to the needs of your organization.

There are several options for deployment of Kaspersky Security Center Linux components on an organization's network, depending on the following criteria:

- Total number of devices
- Units (local offices, branches) that are detached organizationally or geographically
- Separate networks connected by narrow channels
- Need for internet access to the Administration Server

One Administration Server can support a maximum of 50,000 devices (with PostgreSQL or Postgres Pro as the DBMS). If the total number of devices on an organization's network exceeds 50,000, multiple Administration Servers must be deployed on that network and combined into a hierarchy for convenient centralized management.

If an organization includes large-scale remote local offices (branches) with their own administrators, it is useful to deploy Administration Servers in those offices. Otherwise, those offices must be viewed as detached networks connected by low-throughput channels; see article "Standard configuration: A few large-scale offices run by their own administrators".

When detached networks connected with narrow channels are used, traffic can be saved by assigning one or several Network Agents to act as distribution points (see table for calculation of the number of distribution points). In this case, all devices on a detached network retrieve updates from such local update centers. Actual distribution points can download updates both from the Administration Server (default scenario), and from Kaspersky servers on the internet (see article "Standard configuration: Multiple small remote offices").

Section "Standard configurations of Kaspersky Security Center Linux" provides detailed descriptions of the standard configurations of Kaspersky Security Center Linux. When planning the deployment, choose the most suitable standard configuration, depending on the organization's structure.

At the stage of deployment planning, the assignment of the special certificate X.509 to the Administration Server must be considered. Assignment of the X.509 certificate to the Administration Server may be useful in the following cases (partial list):

- Inspecting secure socket layer (SSL) traffic by means of an SSL termination proxy or for using a reverse proxy
- Integration with the public keys infrastructure (PKI) of an organization
- Specifying required values in certificate fields
- Providing the required encryption strength of a certificate

# Selecting the configuration of Kaspersky Security Center Linux

This section describes the following standard configurations used for deployment of Kaspersky Security Center Linux components on an organization's network:

- Single office
- A few large-scale offices, which are geographically detached and run by their own administrators
- Multiple small offices, which are geographically detached

## Standard configuration: Single office

One or several Administration Servers can be deployed on the organization's network. The number of Administration Servers can be selected either based on available hardware, or on the total number of managed devices.

One Administration Server can support up to 50,000 devices (with PostgreSQL or Postgres Pro as the DBMS). Consider the possibility of increasing the number of managed devices in the near future: it may be useful to connect a slightly smaller number of devices to a single Administration Server.

Administration Servers can be deployed either on the internal network, or in the DMZ, depending on whether internet access to the Administration Servers is required.

If multiple Servers are used, it is recommended that you combine them into a hierarchy. Using an Administration Server hierarchy allows you to avoid dubbed policies and tasks, and handle the whole set of managed devices as if they are managed by a single Administration Server (that is, search for devices, build selections of devices, and create reports).

## Standard configuration: A few large-scale offices run by their own administrators

If an organization has a few large-scale, geographically separate offices, you must consider the option of deploying Administration Servers at each of the offices. One or several Administration Servers can be deployed per office, depending on the number of client devices and hardware available. In this case, each of the offices can be viewed as a "Standard configuration: Single office". For ease of administration, it is recommended to combine all of the Administration Servers into a hierarchy (possibly multi-level).

If some employees move between offices with their devices (laptops), create Network Agent connection profiles in the Network Agent policy.

## Standard configuration: Multiple small remote offices

This standard configuration provides for a headquarters office and many remote small offices that may communicate with the HQ office over the internet. Each of the remote offices may be located behind a Network Address Translation (NAT), that is, no connection can be established between two remote offices because they are isolated.

An Administration Server must be deployed at the headquarters office, and one or multiple distribution points must be assigned to all other offices. If the offices are linked through the internet, it may be useful to create a *Download updates to the repositories of distribution points* task for the distribution points, so that they will download updates directly from Kaspersky servers, local or network folder, not from the Administration Server.

If some devices at a remote office have no direct access to the Administration Server (for example, access to the Administration Server is provided over the internet but some devices have no internet access), distribution points must be switched into connection gateway mode. In this case, Network Agents on devices at the remote office will be connected, for further synchronization, to the Administration Server—but through the gateway, not directly.

As the Administration Server, most probably, will not be able to poll the remote office network, it may be useful to turn this function over to a distribution point.

The Administration Server will not be able to send notifications to port 15000 UDP to managed devices located behind the NAT at the remote office. To resolve this issue, you can enable the mode of continuous connection to the Administration Server in the properties of devices acting as distribution points (**Do not disconnect from the Administration Server** check box). This mode is available if the total number of distribution points does not exceed 300. Use push servers to make sure that there is continuous connectivity between a managed device and the Administration Server. Refer to the following article for details: Enabling a push server.

# Selecting a structure for protection of an enterprise

Selection of a structure for protection of an organization is defined by the following factors:

- Organization's network topology.
- Organizational structure.
- Number of employees in charge of the network protection, and allocation of their responsibilities.

- Hardware resources that can be allocated to protection management components.
- Throughput of communication channels that can be allocated to maintenance of protection components on the organizational network.
- Time limits for execution of critical administrative operations on the organization's network. Critical administrative operations include, for example, the distribution of anti-virus databases and modification of policies for client devices.

When you select a protection structure, it is recommended first to estimate the available network and hardware resources that can be used for the operation of a centralized protection system.

To analyze the network and hardware infrastructure, it is recommended that you follow the process below:

1. Define the following settings of the network on which the protection will be deployed:
   - Number of network segments.
   - Speed of communication channels between individual network segments.
   - Number of managed devices in each of the network segments.
   - Throughput of each communication channel that can be allocated to maintain the operation of the protection.
2. Determine the maximum allowed time for the execution of key administrative operations for all managed devices.
3. Analyze information from steps 1 and 2, as well as data from load testing of the administration system. Based on the analysis, answer the following questions:
   - Is it possible to serve all the clients with a single Administration Server, or is a hierarchy of Administration Servers required?
   - Which hardware configuration of Administration Servers is required in order to deal with all the clients within the time limits specified in step 2?
   - Is it required to use distribution points to reduce load on communication channels?

Upon obtaining answers to the questions in step 3 above, you can compile a set of allowed structures of the organization's protection.

On the organization's network you can use one of the following standard protection structures:

- One Administration Server. All client devices are connected to a single Administration Server. Administration Server functions as distribution point.
- One Administration Server with distribution points. All client devices are connected to a single Administration Server. Some of the networked client devices function as distribution points.

- Hierarchy of Administration Servers For each network segment, an individual Administration Server is allocated and becomes part of a general hierarchy of Administration Servers. The primary Administration Server functions as distribution point.

- Hierarchy of Administration Servers with distribution points. For each network segment, an individual Administration Server is allocated and becomes part of a general hierarchy of Administration Servers. Some of the networked client devices function as distribution points.

# Typical schemes of protection system deployment

This section describes the standard deployment schemes of a protection system in an enterprise network using Kaspersky Security Center.

The system must be protected against any type of unauthorized access. We recommend that you install all available security updates for your operating system before installing the application on your device and physically protect Administration Server(s) and distribution point(s).

You can use Kaspersky Security Center to deploy a protection system on a corporate network by means of the following deployment schemes:

- Deploying a protection system through Kaspersky Security Center Web Console.

  Kaspersky applications are automatically installed on client devices, which in turn are automatically connected to the Administration Server by using Kaspersky Security Center.

- Deploying a protection system manually using stand-alone installation packages generated by Kaspersky Security Center.

  Installation of Kaspersky applications on client devices and the administrator's workstation is performed manually; the settings for connecting client devices to the Administration Server are specified when Network Agent is installed.

  This deployment method is recommended in cases when remote installation is not possible.

Kaspersky Security Center does not support deployment using Microsoft Active Directory® group policies.

# Selecting a DBMS

The following table lists the valid DBMS options, as well as the recommendations and restrictions on their use.

Recommendations and restrictions on DBMS

| DBMS | Recommendations and limitations |
| --- | --- |
| MySQL (see supported versions) | Use this DBMS if you intend to run a single Administration Server for less than 20,000 devices. |
| MariaDB (see supported versions) | Use this DBMS if you intend to run a single Administration Server for less than 20,000 devices. |

| | |
|---|---|
| PostgreSQL, Postgres Pro (see supported versions) | Use this DBMS if you intend to run a single Administration Server for less than 50,000 devices. |
| Tantor (see supported versions) | Use this DBMS if you intend to run a single Administration Server for less than 50,000 devices.<br>The Tantor DBMS is only supported on Astra Linux Special Edition RUSB.10015-01 (operational update 1.8). |

For information about how to install the selected DBMS, refer to its documentation.

It is recommended to disable the Software inventory task and disable (in the Kaspersky Endpoint Security policy settings) notifications of Administration Server on started applications.

If you decide to install PostgreSQL or Postgres Pro DBMS, ensure that you specified a password for the superuser. If the password is not specified, Administration Server might not be able to connect to the database.

If you install MySQL, MariaDB, PostgreSQL, or Postgres Pro, use the recommended settings to ensure the DBMS functions properly.

If you use a PostgreSQL, MariaDB or MySQL DBMS, the **Events** tab may display an incomplete list of events for the selected client device. This occurs when the DBMS stores a very large amount of events. You can increase the number of displayed events by doing either of the following:

- Removing unnecessary events.
- Reducing the storage term for unnecessary events.

To see a full list of events logged on the Administration Server for the device, use Reports.

# Providing internet access to Administration Server

The following cases require internet access to the Administration Server:

- Regular updating of Kaspersky databases, software modules, and applications
- Updating third-party software

  By default, internet connection is not required for Administration Server to install Microsoft software updates on the managed devices. For example, the managed devices can download the Microsoft software updates directly from Microsoft Update servers or from Windows Server with Microsoft Windows Server Update Services (WSUS) deployed in your organization's network. Administration Server must be connected to the internet in the following cases:

  - When you use Administration Server as WSUS server
  - To install updates of third-party software other than Microsoft software
- Fixing third-party software vulnerabilities

An internet connection is required for the Administration Server to perform the following tasks:

  - To make a list of recommended fixes for vulnerabilities in Microsoft software. The list is created and regularly updated by Kaspersky specialists.
  - To fix vulnerabilities in third-party software other than Microsoft software.

- Managing devices (laptops) of out-of-office users
- Managing devices in remote offices
- Interacting with primary or secondary Administration Servers located in remote offices
- Mobile Device Management

This section describes typical ways of providing access to the Administration Server over the internet. Each of the cases focusing on providing internet access to the Administration Server may require a dedicated certificate for the Administration Server.

## Internet access: Administration Server on a local network

If the Administration Server is located on the internal network of an organization, you might want to make TCP port 13000 of the Administration Server accessible from outside by means of port forwarding.

## Internet access: Administration Server in DMZ

If the Administration Server is located in the DMZ of the organization's network, it has no access to the organization's internal network. Therefore, the following limitations apply:

- The Administration Server cannot detect new devices.
- The Administration Server cannot perform initial deployment of Network Agent through forced installation on devices on the internal network of the organization.

  This only applies to the initial installation of Network Agent. Any further upgrades of Network Agent or the security application installation can, however, be performed by the Administration Server.

Note that Kaspersky Security Center Linux does not support deployment using group policies of Microsoft Windows.

You can use distribution points located on the organization's network. To perform initial deployment on devices without Network Agent, you first install Network Agent on one of the devices and then assign it the distribution point status. As a result, initial installation of Network Agent on other devices will be performed by the Administration Server through this distribution point.

To ensure a successful sending of notifications to port 15000 UDP on managed devices located on the internal network of the organization, you must cover the entire network with distribution points. In the properties of the distribution points that were assigned, select the **Do not disconnect from the Administration Server** check box. As a result, the Administration Server will establish a continuous connection to the distribution points while they will be able to send notifications to port 15000 UDP on devices that are on the organization's internal network (it can be an IPv4 or IPv6 network).

# Installation

This section describes installation of Kaspersky Security Center Linux and Kaspersky Security Center Web Console.

# Configuring the MariaDB x64 server for working with Kaspersky Security Center Linux

To successfully configure MariaDB x64 server for working with Kaspersky Security Center, you must use the default server parameters except for the server parameters specified in this article.

Recommended settings for the my.cnf file

For more details about DBMS configuring, refer also to the account configuring procedure. For information about DBMS installation, refer to the DBMS installation procedure.

*To configure the my.cnf file:*

1. Open the my.cnf file in a text editor.

2. Enter the following lines into the [mysqld] section of the my.cnf file:

```
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=< 80% of the RAM allocated for the DBMS; see the
documentation of your DBMS for recommendations >
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"
```

Note that the memory specified in the `innodb_buffer_pool_size` value is allocated at server startup. If the database size is smaller than the specified buffer size, only the required memory is allocated. If you use MariaDB 10.4.3 or older, the actual size of allocated memory is approximately 10 percent greater than the specified buffer size. For recommendations on setting the `innodb_buffer_pool_size` and other additional information, see the MySQL documentation.

It is recommended to use the parameter value `innodb_flush_log_at_trx_commit=0`, because the values "1" or "2" negatively affect the operating speed of MariaDB. Ensure that the `innodb_file_per_table` parameter is set to `1`.

For MariaDB 10.1, additionally enter the following lines into the [mysqld] section:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

For MariaDB 10.6, additionally enter the following lines into the [mysqld] section:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

By default, the optimizer add-ons `join_cache_incremental`, `join_cache_hashed`, `join_cache_bka` are enabled. If these add-ons are not enabled, you must enable them.

*To check whether optimizer add-ons are enabled:*

1. In the MariaDB client console, execute the command:

   ```
   SELECT @@optimizer_switch;
   ```

2. Make sure that its output contains the following lines:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   If these lines are present and have the values `on`, then optimizer add-ons are enabled.

   If these lines are missing or have `off` values, you need to do the following:

   a. Open the my.cnf file in a text editor.

   b. Add the following lines into the my.cnf file:

   ```
   optimizer_switch='join_cache_incremental=on'
   optimizer_switch='join_cache_hashed=on'
   optimizer_switch='join_cache_bka=on'
   ```

The add-ons `join_cache_incremental`, `join_cache_hash`, and `join_cache_bka` are enabled.

Increase the default limit of files that can be opened (file descriptors) for the MariaDB systemd service to ensure stability under load.

*To increase the limit of file descriptors:*

1. Execute the following command:

   ```
   sudo systemctl edit mariadb.service
   ```

2. Specify the limit of the file descriptors in the `LimitNOFILE` parameter of the `[Service]` section:

   ```
   LimitNOFILE=1048576
   ```

3. Run the following command to ensure that the parameters are specified correctly:

   ```
   sudo systemd-analyze verify mariadb.service
   ```

4. Run the following command to reload the systemd process:

   ```
   sudo systemctl daemon-reload
   ```

5. Run the following command to restart the MariaDB service:

   `sudo systemctl restart mariadb.service`

   The limit of file descriptors is now increased.

# Configuring a PostgreSQL-based DBMS server to work with Kaspersky Security Center Linux

This article describes how to configure an Administration Server deployed on a single device. If you are using a high-availability DBMS cluster, read the Preparing a high availability DBMS cluster for working with Kaspersky Security Center Linux article.

Kaspersky Security Center Linux supports PostgreSQL-based DBMS. To configure a PostgreSQL database server for working with Kaspersky Security Center Linux, use default settings for the server, except the settings listed in this article.

> The default path to the configuration file is `/etc/postgresql/<VERSION>/main/postgresql.conf`.
> In the ALT Linux operating system, the default path is `/var/lib/pgsql/data/postgresql.conf`

*To prepare the DBMS for the installation of Kaspersky Security Center Linux:*

1. Manage the required settings of the DBMS server in accordance with the documentation of your DBMS.
2. To optimally integrate the DBMS with Kaspersky Security Center Linux, specify the following settings:

   - `max_connections = 151`
   - `shared_buffers = N`

     N = 25% of the estimated RAM sizing for the DBMS. If the DBMS is installed on a device alongside the Administration Server, the calculation should be based on the RAM allocated for the DBMS, not the total RAM of the device.

     If RAM is less than 1 GB, then leave the default value.
   - `temp_buffers = 24MB`
   - `work_mem = 16MB`
   - `maintenance_work_mem = 128MB`
   - `max_stack_depth` = maximum stack size (execute the '`ulimit -s`' command to obtain this value in KB) minus the 1 MB safety margin
   - `max_parallel_workers_per_gather = 0`
   - `standard_conforming_strings = on`

   If you use Postgres Pro 15.7 or Postgres Pro 15.7.1, disable the `enable_compound_index_stats` parameter:
   `enable_compound_index_stats = off`

   Reload the configuration or restart the DBMS server after updating the configuration file by running the following command:

`sudo systemctl restart postgresql-<version>`

or

`sudo systemctl restart postgresql`

3. Create databases and user accounts.

   For instructions on creating databases and setting up user accounts for a PostgreSQL-based DBMS, see the Creating PostgreSQL-based databases and user accounts article.

The DBMS is ready for the installation of Kaspersky Security Center Linux.

# Configuring the MySQL x64 server for working with Kaspersky Security Center Linux

To successfully configure MySQL x64 server for working with Kaspersky Security Center, you must use the default server parameters except for the server parameters specified in this article.

If you use the MySQL server for Kaspersky Security Center, enable support of InnoDB and MEMORY storage and of UTF-8 and UCS-2 encodings.

## Recommended settings for the my.cnf file

For more details about DBMS configuring, refer also to the account configuring procedure. For information about DBMS installation, refer to the DBMS installation procedure.

*To configure the my.cnf file:*

1. Open the my.cnf file in a text editor.

2. Add the following lines to the `[mysqld` section of the my.cnf file:

```
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=< 80% of the RAM allocated for the DBMS; see the
documentation of your DBMS for recommendations >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (in most cases, the server uses small transactions)
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
```

Note that the memory specified in the `innodb_buffer_pool_size` value is allocated at server startup. If the database size is smaller than the specified buffer size, only the required memory is allocated. The actual size of allocated memory is approximately 10 percent greater than the specified buffer size. For recommendations on setting the `innodb_buffer_pool_size` and other additional information, see the MySQL documentation.

It is recommended to use the parameter value `innodb_flush_log_at_trx_commit = 0`, because the values "1" or "2" negatively affect the operating speed of MySQL. Ensure that the `innodb_file_per_table` parameter is set to `1`.

# Preparing a high availability DBMS cluster for working with Kaspersky Security Center Linux

This article describes the steps to prepare a high-availability DBMS cluster for Kaspersky Security Center Linux. If the Administration Server is deployed on a single device, review the Configuring a PostgreSQL-based DBMS server to work with Kaspersky Security Center Linux article.

Kaspersky Security Center Linux supports the following high availability clusters:

- Platform V Pangolin
- Postgres Pro Built-in High Availability
- Patroni (with optional HAProxy load balancer)

A minimum recommended high availability DBMS cluster configuration must include at least three nodes.

*To prepare a high availability DBMS cluster for working with Kaspersky Security Center Linux:*

1. Set the replication type to synchronous.

   If you use the Patroni template version 3.3.1 or earlier for PostgreSQL, ensure that the `synchronous_standby_names` parameter is applied correctly.

   To check that synchronous replication is used, run the following query on the primary node:

   `SELECT application_name, client_addr, client_hostname, client_port, sync_state FROM pg_stat_replication;`

   If the `sync_state` column for any node displays values other than `sync` or `potential`, the cluster uses asynchronous replication, which is not supported. To resolve this issue, do any of the following:

   Update Patroni to version 3.3.2 or newer.

   In the Patroni configuration file, locate the `dcs` sub section of the `bootstrap` section and set the `synchronous_mode` parameter to `true`:

   ```
   bootstrap:
   dcs:
   <...>
   synchronous_mode: true
   ```

2. On each node of the DBMS cluster, set up the configuration file by following steps 1 and 2 of the Configuring a PostgreSQL-based DBMS server to work with Kaspersky Security Center Linux instructions.

3. Create databases and user accounts in accordance with the instructions in the Creating PostgreSQL-based databases and user accounts article.

4. Configure the discovery of DBMS cluster nodes in one of the following ways:

   - Manually specify all nodes of the DBMS cluster during the installation of Kaspersky Security Center Linux.
   - For automatic discovery of cluster nodes, specify only the DNS name or IP address of the control node or replica node during the installation of Kaspersky Security Center Linux.

     To do so:

     a. On all nodes of the high-availability DBMS cluster, add the following line to the `postgresql` configuration file:

     `log_hostname=1`

     b. After editing the configuration file, restart the DBMS cluster service on all high availability DBMS cluster nodes.

     c. Ensure that the database user has the `pg_read_all_stats` privilege.

     You can grant this privilege by running the following command:

     `GRANT pg_read_all_stats TO "<kscdbadmin>";`

     Where `<kscdbadmin>` is the name of the database user.

     The user name of the Administration Server database is specified when installing Kaspersky Security Center Linux.

     d. Configure load balancer for the IAM database.

The high availability DBMS cluster is ready for working with Kaspersky Security Center Linux.

# Installing Kaspersky Security Center Linux

This procedure describes how to install Kaspersky Security Center Linux.

Before installing the application, following these steps:

- Design the deployment of Kaspersky Security Center Linux in accordance with the recommendations of the Getting started scenario.

  If you have satisfied the prerequisites and completed steps 1 through 4 of the scenario, proceed with the installation of the Kaspersky Security Center Linux Administration Server.

  > If you use the operating system RED OS 7.3.4 or later or MSVSPHERE 9.2 or later, install the libxcrypt-compat package for the correct function of Administration Server.

- Install the DBMS for Kaspersky Security Center Linux. You can choose one of supported DBMS.

  If your Linux distribution does not include a supported DBMS, you can install the DBMS from a third-party package repository of the vendor or from another trusted source.

After installing the DBMS, follow the corresponding instruction:

- Configuring a PostgreSQL-based DBMS server to work with Kaspersky Security Center Linux
- Configuring the MariaDB x64 server for working with Kaspersky Security Center Linux
- Configuring the MySQL x64 server for working with Kaspersky Security Center Linux

- Make sure that the DNS server is available on the network.

  Make sure FQDN addresses and DNS names of the server components of Kaspersky Security Center Linux are successfully converted to IP addresses in the operating systems of the application components and on network devices.

- Download the installation file with the necessary localization from the Kaspersky website.

  Choose the installation file that corresponds to the Linux distribution installed on your device—ksc64_<version_number>_amd64.deb or ksc64-<version_number>.x86_64.rpm.

  > The language of the installed Administration Server depends on the localization of the downloaded distribution package.

*To install Kaspersky Security Center Linux:*

1. Create a security group for Kaspersky Security Center services, an unprivileged user for starting the Administration Server services, and an unprivileged user for starting IAM services.

   These users must be members of the Kaspersky Security Center security group.

   To achieve this, run the following commands in sequence (in this example, the security group is "kladmins", the user for running Administration Server services is "ksc", and the user for starting the IAM services is "ksciam"):

   ```
   sudo adduser ksc
   sudo groupadd kladmins
   sudo gpasswd -a ksc kladmins
   sudo usermod -g kladmins ksc
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

2. If necessary, increase the default limit of files that can be opened (file descriptors) for the accounts used for the function of Administration Server services.

   To do this, open the /etc/security/limits.conf file, and then specify the soft and hard limits of the file descriptors as follows:

   ```
   ksc soft nofile <max_number_of_opened_files>
   ksc hard nofile <max_number_of_opened_files>
   ```

   By default, limits of the file descriptors are specified during the installation. The soft file limit is 32 768 files, the hard file limit is 131 072 files.

3. Run the Kaspersky Security Center Linux installation.

   Depending on your Linux distribution, run one of the following commands:

   ```
   sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
   sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm
   ```

4. Run the Kaspersky Security Center Linux initial configuration script:

   `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`

5. Read the End User License Agreement (EULA) and the Privacy Policy. The text is displayed in the command line window. Press the space bar to view the next text segment. Then, when prompted, enter the following values:

   a. Enter `y` if you understand and accept the terms of the EULA. Enter `n` if you do not accept the terms of the EULA. To use Kaspersky Security Center Linux, you must accept the terms of the EULA.

   b. Enter `y` if you understand and accept the terms of the Privacy Policy, and if you agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. Enter `n` if you do not accept the terms of the Privacy Policy. To use Kaspersky Security Center Linux, you must accept the terms of the Privacy Policy.

6. When prompted, enter the following settings:

   a. Select **Standard** as an Administration Server installation mode.

   b. Enter the FQDN or DNS name of the Administration Server. This name will be used by other devices to connect to the Administration Server.

   c. Enter the Administration Server SSL port number. The default port number is 13000.

   d. Evaluate the approximate number of devices that you intend to manage:

      - If you have from 1 to 100 managed devices, enter 1.
      - If you have from 101 to 1000 managed devices, enter 2.
      - If you have more than 1000 managed devices, enter 3.

      This setting is used for automatically randomized delay of task starts to optimize network load. The list below shows the interval within which the delay is calculated:

      - 1 to 100 managed devices, value 1. Delay is not used.
      - 101 to 1000 managed devices, value 2. Delay is 5 minutes.
      - More than 1000 managed devices, value 3. Delay is 10 minutes.

   e. Enter the name of the security group created at step 1 (in the example, the group is `kladmins`).

   f. Enter the name of the user that will start the Administration Server service created at step 1 (in the example, the user is `ksc`).

      The user must be a member of the security group that you specified at step 8e.

   g. Enter the user name that will start other services (in the example, the group is `kladmins`).

      The user must be a member of the security group that you specified at step 8e.

   h. Select the DBMS that you installed to work with Kaspersky Security Center Linux:

      - If you installed MySQL or MariaDB, enter 1.
      - If you have installed a PostgreSQL based DBMS, enter 2.

i. Enter the DNS name or IP address of the device on which the Administration Server database is installed. For local DBMS installation, specify 127.0.0.1.

To use a high availability failover cluster, do one of the following:

- Enter DNS names or IP addresses and ports of all nodes in the following format:

  `<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;`

- Specify only the DNS name or IP address of the primary node, or the replica node.

j. Enter the database port number. This port is used to communicate with Administration Server. This step is skipped if you entered DNS names or IP addresses and ports of all high availability cluster nodes in the step 8i.

By default, the following ports are used:

- Port `3306` for MySQL or MariaDB
- Port `5432` for PostgreSQL or Postgres Pro

k. Enter the name of the Administration Server database (in the example in the articles, the `kav` database) that you created by following the instructions: Creating PostgreSQL-based databases and user accounts or Configuring the MariaDB x64 server for working with Kaspersky Security Center Linux.

l. Enter the name of the database administrator account used to access the Administration Server database (in the example in these articles from step 8k, `kscdbadmin`).

m. Enter the password of the database administrator account that you use for access to the Administration Server database.

n. If you have installed a PostgreSQL-based database, you can specify the database schema to be used by the Administration Server. To do it, specify the schema name.

> The schema name is case-sensitive: you have to use only lowercase letters.

If you do not want to use a custom schema, press ENTER. In this case, the default schema selected in the DBMS is used.

o. Enter the FQDN or DNS name of the IAM server. If you do not specify this variable, the DNS name of the device with Administration Server installed is used.

Enter the value that you specified at step 8b.

p. Enter the name of the account that will start the IAM service created at step 1. The user must be a member of the security group that you specified at step 8e (in the example at step 1, `ksciam`).

q. Select the DBMS that you installed to work with the IAM service:

- If you installed MySQL or MariaDB, enter 1.
- If you installed PostgreSQL or Postgres Pro, enter 2.

r. Enter the IAM DBMS address to be used by the IAM service.

To use a high availability cluster, do one of the following:

- Enter DNS names or IP addresses and ports of all nodes in the following format:
  `<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;`
- Specify only the DNS name or IP address of the load balancer.

s. Enter the IAM DBMS port number. This port is used to communicate with the IAM service. This step is skipped if you entered DNS names or IP addresses and ports of all high availability cluster nodes in the step 8r.

   By default, the following ports are used:

   - Port 3306 for MySQL or MariaDB.
   - Port 5432 for PostgreSQL or Postgres Pro.

t. Enter the IAM database name to be used by the IAM service (in the example, `iam`).

u. Enter the user name of the database administrator account that you use for access to the database (in the example, `iamdbadmin`).

v. Enter the password of the database administrator account that you use for access to the IAM database.

   Wait for the services to be added and started automatically:

   - `klnagent_srv`
   - `kladminserver_srv`
   - `klactprx_srv`
   - `klwebsrv_srv`
   - `kliam_srv`

w. If you installed PostgreSQL or Postgres Pro, you can specify the database schema to be used by IAM. To do it, specify the schema name.

   If you do not want to use a custom schema, press ENTER. In this case, the 'public' schema is used.

   > The schema name is case-sensitive: you have to use only lowercase letters.
   > Do not specify the reserved iam schema names: client, iam, ksc, locker, pat, scope, voltron.

x. Create an account that will act as an Administration Server administrator. Enter the user name and password.

   The password must comply with the following rules:

   - The user password cannot have fewer than 8 or more than 256 characters.
   - The password must contain characters from at least three of the groups listed below:
     - Uppercase letters (A–Z)
     - Lowercase letters (a-z)

- Numbers (0–9)
- Special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

If you skip this step, you can use the following command to create a new user later:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p
```

The user is added and Kaspersky Security Center Linux is installed.

Proceed to installing Kaspersky Security Center Web Console.

If the Administration Server does not have access to the repository of application distribution packages for remote installation, then download the dependencies required to create installation packages for installing applications on Windows devices in the following way:

1. Create the RIUtilsArchiveDirUsed flag by running the following command:

   `/opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1`

2. Download additional modules, "Files for remote installation via Kaspersky Security Center" from the Kaspersky website.

   The downloaded archives have the following names:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Do not rename the archives.

3. Place the archives in the /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives directory.

4. Run the following command to restart the Administration Server service:

   `systemctl restart kladminserver_srv.service`

The Administration Server now has the required dependencies.

## Service verification

Use the following commands to check whether or not a service is running:

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`
- `systemctl status kliam_srv.service`

# Installing Kaspersky Security Center Linux in silent mode

You can install Kaspersky Security Center Linux on Linux devices by using an answer file to run an installation in silent mode, that is, without user participation. The answer file contains a custom set of installation parameters: variables and their respective values.

Before installation:

- Install the DBMS for Kaspersky Security Center Linux. You can choose one of supported DBMS. For information about how to install the selected DBMS, refer to its documentation.

  If the distribution of your Linux-based operating system does not contain a supported DBMS, you can install the DBMS from a third-party package repository.

  After installing the DBMS, follow the corresponding instruction:

  - Configuring the PostgreSQL or Postgres Pro server for working with Kaspersky Security Center Linux

    Configuring the DBMS account for work with PostgreSQL and Postgres Pro

    If you want the Administration Server to automatically discover addresses of cluster nodes, you only need to specify the DNS name or IP address of the control node or the replica node during installation. To do this, make sure that you have completed step 2 of the Preparing a high availability DBMS cluster for working with Kaspersky Security Center Linux instructions.

  - Configuring the MariaDB x64 server for working with Kaspersky Security Center Linux

    Configuring the DBMS account for work with MySQL and MariaDB

  - Configuring the MySQL x64 server for working with Kaspersky Security Center Linux

    Configuring the DBMS account for work with MySQL and MariaDB

- Make sure that your device with the DBMS installed does not have DBMS user accounts with the following names:
  - client
  - iam
  - ksc
  - locker
  - pat
  - scope
  - voltron

- Make sure that the device on which you want to install Kaspersky Security Center Linux is running one of the supported Linux distributions.

  If you use the operating system RED OS 7.3.4 or later or MSVSPHERE 9.2 or later, install the libxcrypt-compat package for the correct function of Administration Server.

- Download the installation file with the necessary localization from the Kaspersky website. Choose the installation file that corresponds to the Linux distribution installed on your device—ksc64_[version_number]_amd64.deb or ksc64-[version_number].x86_64.rpm.

To install Kaspersky Security Center Linux in silent mode:

1. Read the End User License Agreement. Follow the steps below only if you understand and accept the terms of the End User License Agreement.

2. Create a group 'kladmins' and unprivileged accounts 'ksc' and 'ksciam' that must be members of the 'kladmins' group. To do this, sequentially run the following commands under an account with root privileges:

   `adduser ksc`

   `groupadd kladmins`

   `gpasswd -a ksc kladmins`

   `usermod -g kladmins ksc`

   `adduser ksciam`

   `gpasswd -a ksciam kladmins`

   `usermod -g kladmins ksciam`

3. On the DBMS server, create a database for IAM. The database name must be different from the database that you installed to work with Kaspersky Security Center Linux. The Administration Server does not remove the IAM database automatically when uninstalling or moving the server to another device, you must remove the database manually.

   - For PostgreSQL, run the following command:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - For MariaDB, run the following command:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

4. Create the answer file (in TXT format), and add a list of variables in the `VARIABLE_NAME=variable_value` format to the answer file. Add each variable on a separate line. The answer file should include the variables listed in the table below.

5. Set the value of the `KLAUTOANSWERS` environment variable in the root or user environment containing the full name of the answer file including the path, for example, with the following command:

   ```
   export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
   ```

6. Run the Kaspersky Security Center Linux installation in silent mode—depending on your Linux distribution, run one of the following commands:

   In the root environment:

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

```
yum install /<path>/ksc64-[version_number].x86_64.rpm -y
```

   In the user environment:

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

```
sudo -E yum install /<path>/ksc64-[version_number].x86_64.rpm -y
```

7. Create a user to work with Kaspersky Security Center Web Console. To do this, run the following command under an account with root privileges and specify a password at least 8 characters long:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

8. Install Kaspersky Security Center Web Console.

Variables of the answer file used as parameters of Kaspersky Security Center Linux installation in silent mode

| Variable name | Required | Description | Possible values |
|---|---|---|---|
| EULA_ACCEPTED | Yes | Confirms that you understand and accept the terms of the End User License Agreement. | 1 |
| PP_ACCEPTED | Yes | Confirms that you understand and accept the terms of the Privacy Policy. | 1 |
| KLSRV_UNATT_SERVERADDRESS | Yes | The Administration Server DNS-name or static IP address. | DNS name or IP address |
| KLSRV_UNATT_PORT_SRV | No | The Administration Server port number. Optional setting. The default value is 14000. | Port number |
| KLSRV_UNATT_PORT_SRV_SSL | No | The Administration Server SSL port number. Optional setting. The default value is 13000. | Port number |
| KLSRV_UNATT_PORT_KLOAPI | No | The number of the port for working with OpenAPI. Also this port is used for receiving connections from Kaspersky Security Center Web Console. Optional setting. The default value is 13299. | Port number |
| KLSRV_UNATT_PORT_GUI | No | The number of the port for working with the klakaut utility. Optional setting. The default value is 13291. The klakaut utility and a Help system for it are located in the Kaspersky Security Center Linux installation folder.<br>This port is closed by default. If you want to use the klakaut utility to automate the Kaspersky Security Center Linux operation, open the 13291 port by using the klscflag utility. | Port number |
| KLSRV_UNATT_NETRANGETYPE | No | The approximate number of devices that you intend to manage. This setting is used to optimize network load. Optional setting. The default value is 1. | 1 for 1 to 100 managed devices.<br>2 for 101 to 1,000 managed devices.<br>3 for more than 1,000 managed devices. |

| | | | |
|---|---|---|---|
| KLSRV_UNATT_DBMS_TYPE | Yes | The database management system type: MySQL (MariaDB) or Postgres. | mysql<br>or<br>postgres |
| KLSRV_UNATT_DBMS_INSTANCE | Yes | The database server address.<br>To use a PostgreSQL, a Postgres Pro Built-in High Availability cluster, or a Platform V Pangolin DBMS cluster, enter DNS names or IP addresses and ports of all nodes in the following format:<br><fqdn1>:<port>,<fqdn2>:<port>,<...><br><fqdnX>:<port>;<br>Alternatively, if you want to use a Platform V Pangolin DBMS cluster, you can specify only the DNS name or IP address of the primary node, or the replica node, when specifying the DBMS address. | DNS name or static IP address of the database server. |
| KLSRV_UNATT_DBMS_PORT | Yes | Port of the database server. Default value for MySQL (MariaDB) is 3306; default value for Postgres is 5432. | 3306<br>or<br>5432 |
| KLSRV_UNATT_DB_NAME | Yes | The database name. The name of the database must be different from the IAM database name specified in the KLSRV_UNATT_DB_IAM_NAME variable. | kav |
| KLSRV_UNATT_DBMS_LOGIN | Yes | The user name of a user that has access to the database. | |
| KLSRV_UNATT_DBMS_PASSWORD | Yes | The password of a user that has access to the database. | |
| KLSRV_UNATT_DBMS_SCHEMA | No | The custom DBMS schema.<br>If you do not specify a custom schema, Administration Server will use a default one.<br>The schema name is case-sensitive: you have to use only lowercase letters.<br>You can only specify a custom schema if PostgreSQL or Postgres Pro are used as a DBMS. Otherwise, the variable is ignored. | database_schema |
| KLSRV_UNATT_IAM_ADDRESS | Yes | User browsers will be redirected to this address by OpenIDConnect.<br>Enter the IAM Server FQDN. You must use the Administration Server DNS name that was specified in the KLSRV_UNATT_SERVERADDRESS parameter. | FQDN |
| KLSRV_UNATT_KLIAMUSER | Yes | The account name to start the IAM service. The account must be a member of the security group specified in KLSRV_UNATT_KLADMINSGROUP variable. | ksciam |
| KLSRV_UNATT_DBMS_IAM_TYPE | Yes | The IAM database management system type: MySQL (MariaDB) or Postgres. | mysql<br>or<br>postgres |
| KLSRV_UNATT_DBMS_IAM_INSTANCE | Yes | The IAM database server address.<br>To use a PostgreSQL, a Postgres Pro Built-in High Availability cluster, or a Platform V Pangolin DBMS cluster, enter DNS names or IP addresses and ports of all nodes in the following format:<br><fqdn1>:<port>,<fqdn2>:<port>,<...><br><fqdnX>:<port>;<br>Alternatively, if you want to use a Platform V Pangolin DBMS cluster, you can specify only the DNS name or IP address of the primary node, or the replica node, when specifying the DBMS address. | IP address |

| | | | |
|---|---|---|---|
| KLSRV_UNATT_DBMS_IAM_PORT | Yes | The IAM database server port. Default value for MySQL (MariaDB) is 3306; default value for Postgres is 5432. | 3306<br>or<br>5432 |
| KLSRV_UNATT_DBMS_IAM_LOGIN | Yes | The username of a user that has access to the IAM database.<br>If the IAM database type is MySQL (MariaDB) and has both of the following settings:<br>• gtid_mode=ON<br>• gtid_purged=ON\|AUTO<br>ensure that the specified user has either of the following DBMS privileges:<br>• RELOAD<br>• FLUSH_TABLES | |
| KLSRV_UNATT_DBMS_IAM_PASSWORD | Yes | The password of a user that has access to the IAM database. | |
| KLSRV_UNATT_DBMS_IAM_SCHEMA | No | The custom DBMS schema.<br>If you do not specify a custom schema, IAM will use a public one.<br>You can only specify a custom schema if PostgreSQL or Postgres Pro are used as a DBMS. Otherwise, the variable is ignored.<br>The schema name is case-sensitive: you have to use only lowercase letters.<br>Do not specify the reserved iam schema names: client, iam, ksc, locker, pat, scope, voltron. | database_schema |
| KLSRV_UNATT_DB_IAM_NAME | Yes | The IAM database name. The name of the IAM database must be different from the database name specified in the KLSRV_UNATT_DB_NAME variable.<br>Specify a manually created empty database. | iamdb |
| KLSRV_UNATT_KLADMINSGROUP | Yes | The security group name for services. | kladmins |
| KLSRV_UNATT_KLSRVUSER | Yes | The account name to start the Administration Server service. The account must be a member of the security group specified in KLSRV_UNATT_KLADMINSGROUP variable. | ksc |
| KLSRV_UNATT_KLSVCUSER | Yes | The account name to start other services. The account must be a member of the security group specified in KLSRV_UNATT_KLADMINSGROUP variable. | ksc |
| If the Administration Server is to be deployed as a Kaspersky Security Center Linux failover cluster, the answer file must include the following additional variables: | | | |
| KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT | No | The failover cluster configuration. If the parameter is omitted in the answer file, the default value is used.<br>Possible values:<br>0—Failover cluster whose nodes are located in a single data center (default value).<br>2—Geo-distributed failover cluster whose nodes are located in different data centers. | 0<br>or<br>2 |
| KLFOC_UNATT_NODE | Yes | The node number (1 or 2). | 1<br>or<br>2 |
| KLFOC_UNATT_STATE_SHARE_MOUNT_PATH | Yes | The state share mount point. | |
| KLFOC_UNATT_DATA_SHARE_MOUNT_PATH | Yes | The data share mount point. | |

| | | | |
|---|---|---|---|
| KLFOC_UNATT_CONN_MODE | Yes | The failover cluster connectivity mode. | VirtualAdapter or ExternalLoadBalancer |
| In case the KLFOC_UNATT_CONN_MODE variable has VirtualAdapter value, the answer file must include the following additional variables: | | | |
| KLFOC_UNATT_CONN_MODE_VA_NAME | Yes | The virtual network adapter name. | |
| KLFOC_UNATT_CONN_MODE_VA_IPV4 | One of these variables is required | The virtual network adapter IP address. | IP address |
| KLFOC_UNATT_CONN_MODE_VA_IPV6 | | The virtual network adapter IPv6 address. | IPv6 address |

If the Administration Server does not have access to the repository of application distribution packages for remote installation, then download the dependencies required to create installation packages for installing applications on Windows devices in the following way:

1. Create the RIUtilsArchiveDirUsed flag by running the following command:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Download additional modules, "Files for remote installation via Kaspersky Security Center" from the Kaspersky website.

   The downloaded archives have the following names:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Do not rename the archives.

3. Place the archives in the /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives directory.

4. Run the following command to restart the Administration Server service:

   ```
   systemctl restart kladminserver_srv.service
   ```

The Administration Server now has the required dependencies.

## Installing Kaspersky Security Center Linux on Astra Linux in the closed software environment mode

This section describes how to install Kaspersky Security Center Linux on the Astra Linux Special Edition operating system.

Before installation:

- Install a DBMS.
- Download the kaspersky_astra_pub_key.gpg application key.
- Download the ksc64_[version_number]_amd64.deb installation file from the Kaspersky website.

Under an account with root privileges, run the commands provided in this instruction with high integrity and zero confidentiality.

*To install Kaspersky Security Center Linux on a device running Astra Linux Special Edition (update 1.7.2), Astra Linux Special Edition (update 1.6), or Astra Linux Special Edition RUSB.10015-01 (update 1.8):*

1. Open the `/etc/digsig/digsig_initramfs.conf` file, and then specify the following setting:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. In the command line, run the following command to install the compatibility package:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Create a directory for the application key:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Place the application key in the directory created in the previous step:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Update the initial RAM file system image for all kernels of the system:

   ```
   update-initramfs -u -k all
   ```

   Reboot the system.

6. Create a group 'kladmins' and unprivileged accounts 'ksc' and 'ksciam'. The accounts must be members of the 'kladmins' group. To do this, sequentially run the following commands:

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   # adduser ksciam
   # gpasswd -a ksciam kladmins
   # usermod -g kladmins ksciam
   ```

7. Run the Kaspersky Security Center Linux installation:

   ```
   # apt install /<path>/ksc64_[ version_number ]_amd64.deb
   ```

8. Run the Kaspersky Security Center Linux configuration:

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

9. Read the End User License Agreement (EULA) and the Privacy Policy. The text is displayed in the command line window. Press the space bar to view the next text segment. Then, when prompted, enter the following values:

    a. Enter `y` if you understand and accept the terms of the EULA. Enter `n` if you do not accept the terms of the EULA. To use Kaspersky Security Center Linux, you must accept the terms of the EULA.

    b. Enter `y` if you understand and accept the terms of the Privacy Policy, and if you agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. Enter `n` if you do not accept the terms of the Privacy Policy. To use Kaspersky Security Center Linux, you must accept the terms of the Privacy Policy.

10. When prompted, enter the following settings:

    a. Enter the FQDN or DNS name of the Administration Server.

    b. Enter the Administration Server port number. The default port number is 14000.

    c. Enter the Administration Server SSL port number. The default port number is 13000.

    d. Evaluate the approximate number of devices that you intend to manage:

    - If you have from 1 to 100 managed devices, enter 1.
    - If you have from 101 to 1000 managed devices, enter 2.
    - If you have more than 1000 managed devices, enter 3.

    This setting is used for automatically randomized delay of task starts to optimize network load. The list below shows the interval within which the delay is calculated:

    - 1 to 100 managed devices, value 1. Delay is not used.
    - 101 to 1000 managed devices, value 2. Delay is 5 minutes.
    - More than 1000 managed devices, value 3. Delay is 10 minutes.

    e. Enter the security group name for services. By default, the 'kladmins' group is used.

    f. Enter the account name to start the Administration Server service. The account must be a member of the entered security group. By default, the ksc account is used.

    g. Enter the account name to start other services. The account must be a member of the entered security group. By default, the ksc account is used.

    h. Select the DBMS that you installed to work with Kaspersky Security Center Linux:

    - If you installed MySQL or MariaDB, enter 1.
    - If you installed PostgreSQL or Postgres Pro, enter 2.

    i. Enter the IP address of the device on which the database is installed.

j. Enter the database port number. This port is used to communicate with Administration Server. By default, the following ports are used:

- Port 3306 for MySQL or MariaDB.
- Port 5432 for PostgreSQL or Postgres Pro.

k. Enter the database name.

l. Enter the login of the database administrator account that you use to access the database.

m. Enter the password of the database administrator account that you use to access the database.

n. Enter the FQDN or DNS name of the IAM server.

Enter the value that you specified at step 10a.

o. Enter the account name to start the kliam service. The account must be a member of the entered security group.

p. Select the DBMS that you installed to work with the IAM service:

- If you installed MySQL or MariaDB, enter 1.
- If you installed PostgreSQL or Postgres Pro, enter 2.

q. Enter the DBMS address to use by the IAM service.

r. Enter the database port number. This port is used to communicate with the IAM service. By default, the following ports are used:

- Port 3306 for MySQL or MariaDB.
- Port 5432 for PostgreSQL or Postgres Pro.

s. Enter the database name to use by the IAM service. The name of the database used by IAM service should be different from database used by the Administration Server.

t. Enter the login of the database root account that you use to access the IAM database.

u. Enter the password of the database root account that you use to access the IAM database.

Wait for the services to be added and started automatically:

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`
- `kliam_srv`

v. Create an account that will act as an Administration Server administrator. Enter the user name and password.

The password must comply with the following rules:

- The user password must have a minimum of 8, and a maximum of 256, characters.
- The password must contain characters from at least three of the groups listed below:
  - Uppercase letters (A–Z)
  - Lowercase letters (a-z)
  - Numbers (0–9)
  - Special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Kaspersky Security Center Linux is installed and the user is added.

To download the dependencies required to create application installation packages for Windows devices:

1. Create the RIUtilsArchiveDirUsed flag by running the following command:
   `/opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1`
2. Download additional modules, "Files for remote installation via Kaspersky Security Center" from the Kaspersky website.
   The downloaded archives have the following names:
   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Do not rename the archives.
3. Place the archives in the /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives directory.
4. Run the following command to restart the Administration Server service:
   `systemctl restart kladminserver_srv.service`

The Administration Server now has the required dependencies.

Service verification

Use the following commands to check whether or not a service is running:

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`

- `# systemctl status klwebsrv_srv.service`
- `# systemctl status kliam_srv.service`

# Installing Kaspersky Security Center Web Console

This section describes how to install Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) on devices running the Linux operating system. Before installation, you must install a DBMS and the Kaspersky Security Center Linux Administration Server.

> If you install Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode, follow the instructions specific for Astra Linux.

Use one of the following installation files that corresponds to the Linux distribution installed on your device:

- For Debian: ksc-web-console-<build number>.x86_64.deb
- For RPM-based operating systems: ksc-web-console-<build number>.x86_64.rpm

You receive the installation file by downloading it from the Kaspersky website.

*To install Kaspersky Security Center Web Console:*

1. Make sure that the device on which you want to install Kaspersky Security Center Web Console is running one of the supported Linux distributions.
2. Read the End User License Agreement. If the Kaspersky Security Center Linux distribution kit does not include a TXT file with the text of EULA, you can download the file from the Kaspersky website. If you do not accept the terms of the License Agreement, do not install the application.
3. Create a response file that contains parameters for connecting Kaspersky Security Center Web Console to the Administration Server: `/etc/ksc-web-console-setup.json`.

   **Example of a response file containing the minimum set of parameters**

The set of parameters of the response file depends on the version of the Administration Server to which the Kaspersky Security Center Web Console connects:

- Administration Server version 16 or later

  Example of a response file with the minimum set of parameters for signing in to Administration Server version 16 or later:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Administration Server version 15.4 or later

  Example of a response file with the minimum set of parameters for signing in to Administration Server version 15.4 or earlier:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

You can install Kaspersky Security Center Web Console either on the same device as Administration Server or on a different device. If Kaspersky Security Center Web Console is installed on a different device, the Kaspersky Security Center Web Console address (specified by `address`) and the Administration Server address (specified by `iamHost` or `kscHost`) differ. If Kaspersky Security Center Web Console is installed on the same device as Administration Server, these parameters have the same values.

The `iamHost` value must match the IAM address that you specified when installing Administration Server. To obtain the specified IAM address, run the following command on the device with Administration Server installed:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

For detailed information, refer to the article: Kaspersky Security Center Web Console installation parameters.

You can add multiple Administration Servers of different versions to the list of trusted servers. In this case, the Servers may use different authentication methods.

We recommend that you specify port numbers above 1024. If you want Kaspersky Security Center Web Console to work on ports below 1024, after installation you have to make sure that you have the setcap utility, and then run the following command:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

If you do not have the setcap utility, you can install it. **Click this link to view the commands.**

For Debian and Ubuntu operating systems, run one of the following commands:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

For SUSE Linux Enterprise Server and Red Hat Enterprise Linux, run the command:

- `sudo zypper install libcap-progs`

When you install Kaspersky Security Center Web Console on ALT Linux operating system, you must specify a port number other than 8080, because port 8080 is used by the operating system.

Kaspersky Security Center Web Console cannot be updated by using the same .rpm installation file. If you want to change the settings in a response file and use this file to reinstall the application, you must first remove the application, and then install it again with the new response file.

4. Under an account with root privileges, use the command line to run the setup file with the .deb or .rpm extension, depending on your Linux distribution.

   - To install or upgrade Kaspersky Security Center Web Console from a .deb file, run the following command:
     `sudo apt-get install ksc-web-console-<build number>.x86_64.deb`
   - To install Kaspersky Security Center Web Console from an .rpm file, run one of the following commands:
     `sudo yum install ksc-web-console-<build number>.x86_64.rpm`

     or

     `sudo alien -i ksc-web-console-<build number>.x86_64.rpm`
   - To upgrade from a previous version of Kaspersky Security Center Web Console, run one of the following commands:
     - For devices running RPM-based operating system:
       `sudo yum install ksc-web-console-<build number>.x86_64.rpm`
     - For devices running Debian-based operating system:
       `sudo apt-get install ksc-web-console-<build number>.x86_64.deb`

   This starts unpacking of the setup file. Please wait until the installation is complete. Kaspersky Security Center Web Console is installed to the following directory: /var/opt/kaspersky/ksc-web-console.

5. Restart all of the Kaspersky Security Center Web Console services by running the following command:
   `sudo systemctl restart KSC*`

When the installation is complete, you can use your browser to open and log in to Kaspersky Security Center Web Console.

If the Administration Server common certificate is replaced with another certificate from a backup, or replaced by using the klsetsrvcert utility, you have to remove, and then reinstall Kaspersky Security Center

Web Console. Otherwise, signing in to Web Console will be restricted.
If after reinstallation you cannot sign in to Web Console, check the IAM Server configuration.

## Kaspersky Security Center Web Console installation parameters

For installing Kaspersky Security Center Web Console Server on devices running Linux, you must create a response file—a .json file that contains parameters for connecting Kaspersky Security Center Web Console to the Administration Server. You must name this file ksc-web-console-setup.json and place it in the /etc/ksc-web-console-setup.json directory.

Administration Server includes Identity and Access Manager (IAM) that provides domain authentication with single sign-on (SSO) in Kaspersky Security Center Web Console. For Kaspersky Security Center Web Console to connect to Administration Server, the response file must contain the parameters for interacting with the IAM component, even if you do not use single sign-on (SSO).

Example of the response file for installing Web Console that will connect to Administration Server version 16 or later. In this example, Web Console and Administration Server are installed on different devices:

```
{
    "webConsoleAddress": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v16": {
    "iamHost": "ksc16.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
    "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "internalCertsTTLDays": 1095,
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "natsMessageQueueAccount": "Group1:User6"
}
```

The `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, `natsMessageQueueAccount`, `certPath`, and `keyPath` parameters are optional. You can omit these parameters in the response file.

If you want to use a custom certificate, specify both the `certPath` and `keyPath` parameters. If you do not specify the parameters or specify only one, the web browser keeps informing you that your connection is not private.

For security reasons, we do not recommend specifying the `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, and `natsMessageQueueAccount` parameters.
If you decide to specify these parameters, make sure that the user accounts that you are configuring belong to the same security group. When the parameters are not specified, the Kaspersky Security Center Web Console installer creates a default security group, and then creates user accounts with default names in this group.
The `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, and `natsMessageQueueAccount` parameters must not be used separately from each other: specify the values either for all of these parameters, or for none of them.

You can install Kaspersky Security Center Web Console either on the same device as Administration Server or on a different device. If Kaspersky Security Center Web Console is installed on a different device, the Kaspersky Security Center Web Console address (specified by `webConsoleAddress`) and the Administration Server address (specified by `iamHost` or `kscHost`) differ. If Kaspersky Security Center Web Console is installed on the same device as Administration Server, these parameters have the same values.

The `iamHost` value must match the IAM address specified when installing the Administration Server. To obtain the specified IAM address, run the following command on the device with Administration Server installed:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

We recommend that you specify port numbers above 1024. If you want Kaspersky Security Center Web Console to work on ports below 1024, after installation you have to run the following command:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

If you do not have the setcap utility, you can install it. **Click this link to view the commands**.

For Debian and Ubuntu operating systems, run one of the following commands:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

For SUSE Linux Enterprise Server and Red Hat Enterprise Linux, run the command:

- `sudo zypper install libcap-progs`

When you install Kaspersky Security Center Web Console on ALT Linux operating system, you must specify a port number other than 8080, because port 8080 is used by the operating system.

The table below describes the parameters that can be specified in a response file.

Parameters for installing Kaspersky Security Center Web Console on devices running Linux

| Setting | Description | Available values |
|---|---|---|
| `webConsoleAddress` | Address of the device (FQDN or host name) where Kaspersky Security Center Web Console is installed (required).<br>If you install Kaspersky Security Center Web Console on Kaspersky Security Center Server, use the address that you specified when installing Kaspersky Security Center Linux.<br>If you install Kaspersky Security Center Web Console on a different device, specify the device address (FQDN or host name) to be used by the web browser for connecting to Kaspersky Security Center Web Console Server. | String value.<br>Example: `"ksc.example.com"` |
| `port` | Port used by Kaspersky Security Center Web Console to receive connections from web browsers (required). | Numerical value.<br>The recommended value is 8080 (except Linux operating system). |
| `defaultLangId` | Language of user interface (by default, `1033`).<br>If necessary, you can change the language of Kaspersky Security Center Web Console interface. | Numerical code of the language:<br>• German: `1031`<br>• English: `1033`<br>• Spanish: `1034`<br>• Spanish (Mexico): `2058`<br>• French: `1036`<br>• Italian: `1040`<br>• Japanese: `1041`<br>• Kazakh: `1087`<br>• Polish: `1045`<br>• Portuguese (Brazil): `1046`<br>• Russian: `1049`<br>• Turkish: `1055`<br>• Simplified Chinese: `2052`<br>• Traditional Chinese: `1028`<br>If no value is specified, then English (en-U used. |
| `enableLog` | Whether or not to enable Kaspersky Security Center Web Console trace logging.<br>We recommend that you change the default value for the parameter only if a Kaspersky Technical Support specialist requests. | Boolean value:<br>• `true`—Logging is enabled.<br>• `false`—Logging is disabled (selecte |

| Setting | Description | Available values |
| --- | --- | --- |
| `trusted` | List of addresses of trusted Administration Servers that Kaspersky Security Center Web Console can connect to. You can add multiple Administration Servers of different versions to the list of trusted servers.<br>For Administration Server version 16 or later:<br>• Administration Server name that will be displayed in the login window.<br>• `iamHost` is the address (FQDN or host name) of the Administration Server, which includes the IAM component (starting with Kaspersky Security Center Linux version 16), and to which Kaspersky Security Center Web Console connects. The `iamHost` value must match the IAM address specified when installing the Administration Server. To obtain the specified IAM address, run the following command on the device with Administration Server installed: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`<br>• `iamOAuthPort` is the port that is used for exchanging authentication tokens over the OpenID Connect authentication protocol (default value is 4444). This port is used both for communication between Kaspersky Security Center Web Console Server and Administration Server, and between the browser (used with Kaspersky Security Center Web Console) and Administration Server.<br>• `iamProxyPort` is the port that is used for connecting Kaspersky Security Center Web Console Server to Administration Server (default value is 9050).<br>• `iamCertPath` is the path to the IAM certificate. The IAM certificate is created automatically the first time you run Administration Server. The certificate is located on the device where Administration Server is installed. The default path to the certificate: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem. The self-signed IAM certificate is rotated automatically.<br>• `iamPATPath` is the path to the token used for registration of Kaspersky Security Center Web Console as an OAuth-client in IAM. This file is generated automatically the first time you run Administration Server. The token is located on the device where Administration Server is installed. The default path to the token: /var/opt/kaspersky/klnagent_srv/iam/initial_token.txt. The token is valid indefinitely and does not require rotation.<br>• `kscPort` is the port that is used for connecting Kaspersky Security Center Web Console to Administration Server over OpenAPI (default value is 13299).<br>• `kscCertPath` is the path to the Administration Server certificate. The certificate is located on the device where Administration Server is installed. The default path to the certificate: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer.<br>For Administration Server version 15.4 or earlier:<br>• Administration Server name that will be displayed in the login window.<br>• `kscHost` is the address (FQDN or host name) of the Administration Server that Kaspersky Security Center Web Console connects to.<br>• `kscPort` is the OpenAPI port that is used for connecting Kaspersky Security Center Web Console Server to Administration Server (default value is 13299).<br>• `kscCertPath` is the path to the Administration Server certificate. The certificate is located on the device where Administration Server is installed. The default path to the certificate: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer.<br>When installing Kaspersky Security Center Web Console on a device other than the Administration Server device, copy the Administration Server certificate file (specified by `kscCertPath`), the IAM certificate file (specified by `iamCertPath`), and the token file (specified by `iamPATPath`) from the device with Administration Server installed to the target device. Specify the local path to these files in the response file for the Web Console installer. | A section of the JSON file in the following<br>`"trusted": { "Administration Server v16": { "iamHost": "ksc-iam.example.com", "iamOAuthPort": 4444, "iamProxyPort": 9050, "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_c "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initia "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ }, "Administration Server v15.4": { "kscHost": "ksc.example.com", "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ } }`<br>You can specify any Administration Serve instead of `Administration Server v1` `Administration Server v15.4`. |

| Setting | Description | Available values |
| --- | --- | --- |
| | | |
| `acceptEula` | Whether or not you want to accept the terms of the End User License Agreement (EULA). The file containing the terms of the EULA is downloaded together with the installation file. | Boolean value:<br>• `true` — I confirm that I have fully read and accept the terms and conditions User License Agreement.<br>• `false` — I do not accept the terms of Agreement (selected by default).<br>If no value is specified, the Kaspersky Sec Web Console installer shows you the EUL whether or not you agree to accept the t EULA. |
| `certDomain` | If you want to generate a new self-signed certificate, use this parameter to specify the FQDN for connecting browser to Kaspersky Security Center Web Console. | String value. |
| `certPath` | Use the parameter to specify the path to the Kaspersky Security Center Web Console custom certificate that is trusted in your infrastructure and meets the requirements for custom certificates.<br>You can specify only one private key (`keyPath`) for one certificate or for a certificate chain. | String value.<br>Encrypted certificates are not supported Security Center Web Console.<br>On the device where Kaspersky Security Console is to be installed, specify the pat certificate file in the PEM encoding forma<br>Example: `/root/server.crt` |
| `keyPath` | Use the parameter to specify the path to the private key associated with the Kaspersky Security Center Web Console custom certificate specified in `certPath` parameter. | String value.<br>The file with the private key must not be e<br>On the device where Kaspersky Security Console is to be installed, specify the pat in the PEM encoding format.<br>Example: `/root/key-without-passph` |
| `webConsoleAccount` | Name of the account under which the Kaspersky Security Center Web Console service is run. | String value in the following format: `"< gr < user name >"`.<br>Example: `"Group1:User1"`.<br>If no value is specified, the Kaspersky Sec Web Console installer creates a new acc default name `user_management_%uid%` |
| `managementServiceAccount` | Name of the account under which the Kaspersky Security Center Web Console Management Service is run. | String value in the following format: `"< gr < user name >"`.<br>Example: `"Group1:User2"`.<br>If no value is specified, the Kaspersky Sec Web Console installer creates a new acc default name `user_nodejs_%uid%`. |
| `serviceWebConsoleAccount` | Name of the account under which the Kaspersky Security Center Web Console service is run. | String value in the following format: `"< gr < user name >"`.<br>Example: `"Group1:User3"`.<br>If no value is specified, the Kaspersky Sec Web Console installer creates a new acc default name `user_svc_nodejs_%uid%` |
| `pluginAccount` | Name of the account under which the Kaspersky Security Center Product Plugins service is run. | String value in the following format: `"< gr < user name >"`.<br>Example: `"Group1:User4"`.<br>If no value is specified, the Kaspersky Sec Web Console installer creates a new acc default name `user_web_plugin_%uid%` |
| `natsMessageQueueAccount` | Name of the account under which the Kaspersky Security Center Web Console NATS service is run. | String value in the following format: `"< gr < user name >"`.<br>Example: `"Group1:User6"`.<br>If no value is specified, the Kaspersky Sec Web Console installer creates a new acc default name `user_message_queue_%u` |
| `internalCertsTTLDays` | Validity term of Kaspersky Security Center Web Console internal certificates. | Optional setting. The default value is 109 |

# Installing Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode

This section describes how to install Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) on the Astra Linux Special Edition operating system. Before installation, you must install a DBMS and the Kaspersky Security Center Linux Administration Server.

*To install Kaspersky Security Center Web Console:*

1. Make sure that the device on which you want to install Kaspersky Security Center Web Console is running one of the supported Linux distributions.

2. Read the End User License Agreement. If the Kaspersky Security Center Linux distribution kit does not include a TXT file with the text of EULA, you can download the file from the Kaspersky website. If you do not accept the terms of the License Agreement, do not install the application.

3. Create a response file that contains parameters for connecting Kaspersky Security Center Web Console to the Administration Server: `/etc/ksc-web-console-setup.json`.

   **Example of a response file containing the minimum set of parameters**

   The set of parameters of the response file depends on the version of the Administration Server to which the Kaspersky Security Center Web Console connects:

   - Administration Server version 16 or later

     Example of a response file with the minimum set of parameters for signing in to Administration Server version 16 or later:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Administration Server version 15.4 or later

  Example of a response file with the minimum set of parameters for signing in to Administration Server version 15.4 or earlier:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

You can install Kaspersky Security Center Web Console either on the same device as Administration Server or on a different device. If Kaspersky Security Center Web Console is installed on a different device, the Kaspersky Security Center Web Console address (specified by `address`) and the Administration Server address (specified by `iamHost` or `kscHost`) differ. If Kaspersky Security Center Web Console is installed on the same device as Administration Server, these parameters have the same values.

The `iamHost` value must match the IAM address that you specified when installing Administration Server. To obtain the specified IAM address, run the following command on the device with Administration Server installed:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

For detailed information, refer to the article: Kaspersky Security Center Web Console installation parameters.

You can add multiple Administration Servers of different versions to the list of trusted servers. In this case, the Servers may use different authentication methods.

4. Open the `/etc/digsig/digsig_initramfs.conf` file, and then specify the following setting:

```
DIGSIG_ELF_MODE=1
```

5. In the command line, run the following command to install the compatibility package:

```
apt install astra-digsig-oldkeys
```

6. Create a directory for the application key:

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

7. Place the application key `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` in the directory created in the previous step:

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

If the Kaspersky Security Center Linux distribution kit does not include the kaspersky_astra_pub_key.gpg application key, you can download it by clicking the link: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Update the RAM disks:

```
update-initramfs -u -k all
```

Reboot the system.

9. Under an account with root privileges, use the command line to run the setup file. You receive the installation file by downloading it from the Kaspersky website.

- To install or upgrade Kaspersky Security Center Web Console, run the following command:

```
sudo apt-get install ksc-web-console-<build_number>.x86_64.deb
```

- To upgrade from a previous version of Kaspersky Security Center Web Console, run the following command:

```
sudo apt-get install ksc-web-console-<build_number>.x86_64.deb
```

This starts unpacking of the setup file. Please wait until the installation is complete. Kaspersky Security Center Web Console is installed to the following directory: `/var/opt/kaspersky/ksc-web-console`.

10. Restart all of the Kaspersky Security Center Web Console services by running the following command:

```
sudo systemctl restart KSC*
```

When the installation is complete, you can use your browser to open and log in to Kaspersky Security Center Web Console.

# Installing Kaspersky Security Center Linux with a script

The `ksc_fast_install.py` script allows you to deploy Kaspersky Security Center Linux and perform the initial setup of its components: Administration Server and Web Console, including DBMS and required support packages.

The script reads parameters from the parameter file. The default values of parameters are used. If necessary, you can change the values.

How the script works

While running, the script:

- Checks if the conditions are met:
  - You have the required rights for script execution.
  - The script is compatible with operating system and DBMS.
  - EULAs and Privacy Policy are accepted.
    If you do not accept them in the parameter file, you will be prompted to do it after running the script.
  - Hardware requirements for Administration Server and Web Console.
    The requirements are defined in the Sizing Guide.
- Installs DBMS (if not yet installed) and configures its parameters
- Creates Kaspersky Security Center databases, configures OS credentials
- Installs Administration Server, Web Console
- Provides you login and password for signing in to Web Console.
  Before you close the command-line terminal, save the credentials in any convenient way. If you lose the credentials, you have to add a new user account by running the command:
  `` `/opt/kaspersky/ksc64/sbin/kladduser -n <user>` ``

If one or several conditions are not met or an error occurs, the script is terminated, and a corresponding notification is displayed.

> The script does not include actions for system hardening. To reduce the risk of Kaspersky Security Center compromise, consider the Hardening guide recommendations.
> Script-based installation method is applicable for deploying Kaspersky Security Center Linux version 16.3 and later on a device with no Kaspersky Security Center Linux.
> Python 3.6 or later is required to run the script.

Deployment is only possible if the current device has no Kaspersky Security Center Linux installed.

You cannot use the script to upgrade to a new version of Kaspersky Security Center Linux, or if Kaspersky Security Center Linux failover cluster is deployed.

The `ksc_fast_install.py` script supports installation of Kaspersky Security Center Linux on the operating systems versions with DBMSs described in the table.

| Operating system version | DBMS |
|---|---|
| Ubuntu Server 26.04 LTS | PostgreSQL 18<br>MySQL 8.4 (build 8.4.10) |
| RED OS 8 | PostgreSQL 16<br>MariaDB 10.11 (build 10.11.18) |

| | |
|---|---|
| Astra Linux Special Edition RUSB.10015-01 (operational update 1.8.5) | PostgreSQL 15<br>MariaDB 10.11 (build 10.11.13) |
| CentOS Stream 10 | PostgreSQL 18<br>MariaDB 10.11 (build 10.11.13) |

Custom database schema is not supported by the script.

## How to perform deployment via the script

**Prerequisites**

Before running the script, make sure that you have done the following:

- Update your operating system by executing one of the commands: `dnf update` or `apt update`
- Get the superuser privileges by executing the command: `sudo -i`
- Allow running the script by executing the command: `chmod +x ./ksc_fast_install.py`
- Ensure that repository of your operating system hosts the supported DBMS by executing the command: `sudo apt policy postgresql`

*To deploy Kaspersky Security Center Linux by running the script:*

1. From Kaspersky website, download the following:
   - .deb or .rpm distribution packages for Administration Server and Web Console.
   - The "KSC installation script" archive.

     When using the script, select the Administration Server and Web Console distribution packages that are compatible with your operating system's package manager.

     The archive contains the following files:
     - `ksc_fast_install.py` script file.
     - Parameter file.

       The default file name is `params.txt`. If you want to rename the file, make sure that you specified the new name via the `--params` parameter when running the script in the command-line terminal.
     - File with EULA and Privacy Policy for Administration Server.
     - File with EULA for Kaspersky Security Center Web Console.
     - Files with hash sums for the EULAs.
2. Place all the downloaded files in the same local directory.
3. If necessary, configure the parameter file.

**Click here to view the example of parameter file with the description of its parameters**

```
# Required parameters:

#klfi_server_eula_accepted=N

#klfi_nwc_eula_accepted=N

#klfi_pp_accepted=N

# Optional parameters:

#klfi_klserver_db=KAV

#klfi_klserver_dbuser=klserver

#klfi_klserver_address=

#klfi_kliam_db=KAV_IAM

#klfi_kliam_dbuser=kliam

#klfi_kliam_address=

#klfi_sys_group_kladmin=kladmins

#klfi_sys_user_klserver=klsrvuser

#klfi_sys_user_kliam=kliamuser

#klfi_sys_user_svc=klsvcuser

#klfi_nwc_port=8080

#klfi_display_name=

#klfi_netsize=M
```

The `klfi_server_eula_accepted=N`, `klfi_nwc_eula_accepted=N`, and `klfi_pp_accepted=N` parameters are mandatory and always present in the parameter file. The other parameters are optional.

For mandatory parameters:

- If you change the default value without uncommenting a line, you will be prompted to accept EULA and Privacy Policy.
- If you specify a value other than `Y` or `N`, you will be prompted to accept EULA and Privacy Policy no matter if you uncommented the line.
- If you uncomment the line without changing the default `N` value, the script will not work.
- If you uncomment the line and set the `Y` value, the script will not prompt you.

| Parameter and its default value | Parameter description and other possible values (if any) |
| --- | --- |
| `klfi_server_eula_accepted=N` | End User License Agreement for Administration Server.<br>Possible values:<br>• `Y` – EULA accepted.<br>• `N` – EULA not accepted. |
| `klfi_nwc_eula_accepted=N` | End User License Agreement for Kaspersky Security Center Web Console.<br>Possible values:<br>• `Y` – EULA accepted.<br>• `N` – EULA not accepted. |
| `klfi_pp_accepted=N` | Privacy Policy.<br>Possible values:<br>• `Y` – Privacy Policy accepted.<br>• `N` – Privacy Policy not accepted. |
| `klfi_klserver_db=KAV` | The Administration Server database name.<br>The name must be different from the IAM database name specified in the `klfi_kliam_db` parameter. |
| `klfi_kliam_db=KAV_IAM` | The IAM database name.<br>The name must be different from the Administration Server database name specified in the `klfi_klserver_db` parameter. |
| `klfi_klserver_dbuser=klserver` | Name of the Administration Server database user. |
| `klfi_kliam_dbuser=kliam` | Name of the IAM database user. |
| `klfi_klserver_address=FQDN` | The Administration Server FQDN or the current device name.<br>If the parameter value is not specified, the script automatically defines FQDN or the name of the device on which you run the script.<br>If the script fails to define the values, the installation completes with an error. |
| `klfi_kliam_address=FQDN` | The IAM Server FQDN or the current device name.<br>If the parameter value is not specified, the script automatically defines FQDN or the name of the device on which you run the script.<br>If the script fails to define the values, the installation completes with an error. |
| `klfi_sys_group_kladmin=kladmins` | The security group name for services. |
| `klfi_sys_user_klserver=klsrvuser` | The account name to start the Administration Server service. |
| `klfi_sys_user_kliam=kliamuser` | The account name to start the IAM service. |
| `klfi_sys_user_svc=klsvcuser` | The account name to start other services. |
| `klfi_nwc_port=8080` | Port for connection to Kaspersky Security Center Web Console. |
| `klfi_display_name=FQDN` | Administration Server name that will be displayed in the login window. |

| | |
|---|---|
| `klfi_netsize=M` | The approximate number of devices that you intend to manage.<br>Each estimate accounts for the resources required to run Kaspersky applications. The calculation covers the simultaneous operation of the Administration Server, Network Agent, Kaspersky Security Center Web Console, and Kaspersky Endpoint Security for Linux on a single device.<br>Storage for Administration Server backups is not included in these calculations. Use an external file resource as a mount point to store backups on a separate device, or increase the available disk space to account for backup storage.<br>We recommend adding an additional 4–6 GB of RAM and 20 GB of free disk space for the operating system installation.<br>Hardware resource estimation by network size:<br>• `S` –1 to 1000 managed devices.<br>  • CPU–8 cores<br>  • RAM–16 GB<br>  • Available disk space for the `/var` directory–70 GB, 300 IOPS or higher<br>• `M` –1001 to 10000 managed devices.<br>  • CPU–12 cores<br>  • RAM–24 GB<br>  • Available disk space for the `/var` directory–340 GB, 300 IOPS or higher<br>• `L` –10001 to 30000 managed devices.<br>  • CPU–20 cores<br>  • RAM–40 GB<br>  • Available disk space for the `/var` directory–490 GB, 300 IOPS or higher<br>• `XL` –30001 to 50000 managed devices.<br>  • CPU–28 cores<br>  • RAM–54 GB<br>  • Available disk space for the `/var` directory–640 GB, 300 IOPS or higher |

The parameter file lines are commented. If you want to configure the values, remove the # symbol at the beginning of the line you want to uncomment.

The `klfi_server_eula_accepted`, `klfi_nwc_eula_accepted`, and `klfi_pp_accepted`parameters are mandatory, and their default value is `N`. If you run the script without changing these values in the settings file, you will be prompted to accept the End User License Agreement and the Privacy Policy.

4. Run the script.

After the script is executed, a notification about a successful deployment of Kaspersky Security Center Linux components is displayed, as well as login and password for signing in to the Web Console.

If the conditions for the script-based installation are not met, unknown parameters are specified in the parameter file, or if a parameter is repeated multiple times, the script returns an error, and a corresponding notification is displayed.

If the script incorrectly detects insufficient RAM during the resource discovery step, disable dynamic RAM usage for the duration of the installation.

If an error occurs while installing Kaspersky Security Center Linux components or DBMS, the script rolls back the changes, and then terminates.

Unsuccessful installation rollback

If an error occurs while installing Kaspersky Security Center Linux components or DBMS, the rollback is performed automatically by the script. The component or DBMS installed before the error occurred is deleted.

Upgrade of operating system packages and installation of support packages are not rolled back.

If you manually terminate the script, the successfully completed steps are not rolled back. The next time you run the script (using the `python3 ksc_fast_install.py` command), the installation resumes from the step at which it was interrupted. If you do not want to resume the installation, run the script with the `rollback`: `python3 ksc_fast_install.py rollback.` option. This makes the script roll back all actions performed before it was stopped.

# Deployment of the Kaspersky Security Center Linux failover cluster

A Kaspersky Security Center Linux failover cluster provides high availability of Kaspersky Security Center Linux and minimizes downtime of Administration Server in case of a failure. The failover cluster is based on two identical instances of Kaspersky Security Center Linux installed on two computers. One of the instances works as an active node and the other one is a passive node. The active node manages protection of the client devices, while the passive one is prepared to take all of the functions of the active node in case the active node fails. When a failure occurs, the passive node becomes active and the active node becomes passive.

The Kaspersky Security Center Linux failover cluster supports two configurations:

- A failover cluster whose nodes are located in a single data center.
- A geo-distributed failover cluster whose nodes are located in different data centers.

In a Kaspersky Security Center Linux failover cluster, all Kaspersky Security Center Linux services are managed automatically. Do not try to restart the services manually.

Use the syslog feature for troubleshooting.

### Switch conditions

The failover cluster switches protection management of the client devices from the active node to the passive one, if any of the following events occurs on the active node:

- The active node is broken due to a software or hardware failure.
- The active node was temporarily stopped for maintenance activities.
- At least one of the Kaspersky Security Center Linux services (or processes) failed or incidentally terminated. The Kaspersky Security Center Linux services are the following ones: klnagent_klfoc, kladminserver_klfoc, klactprx_klfoc, klwebsrv_klfoc.
- The network connection between the active node and the storage on the file server was interrupted or terminated (only for the cluster located in a single data center).

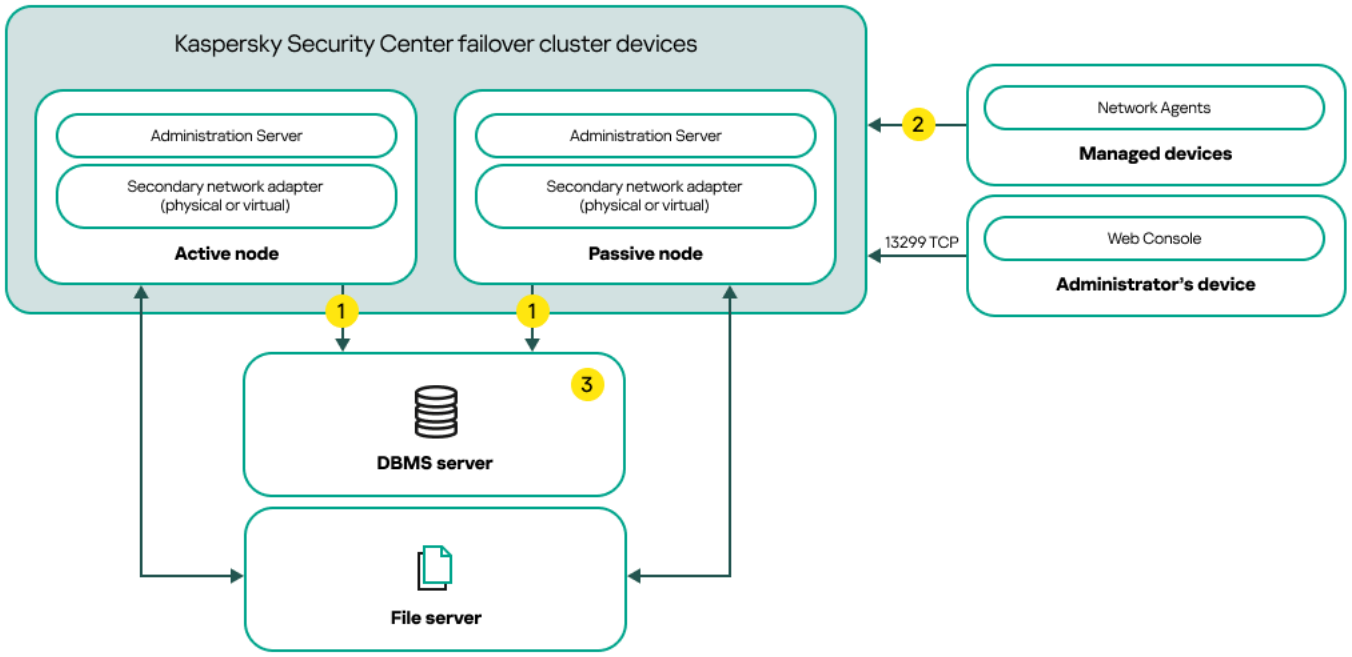
## Kaspersky Security Center Linux failover cluster. Deployment schemes

You can choose one of the following schemes to deploy the Kaspersky Security Center Linux failover cluster:

- Kaspersky Security Center Linux failover cluster deployed within a single data center:
  - A scheme that uses a secondary network adapter and a DBMS installed on a dedicated device.
  - A scheme that uses a third-party load balancer and a DBMS installed on a dedicated device.
- Geo-distributed Kaspersky Security Center Linux failover cluster deployed across multiple data centers.

Kaspersky Security Center Linux failover cluster

A scheme that uses a secondary network adapter and a DBMS installed on a dedicated device




A scheme that uses a secondary network adapter and a DBMS installed on a dedicated device

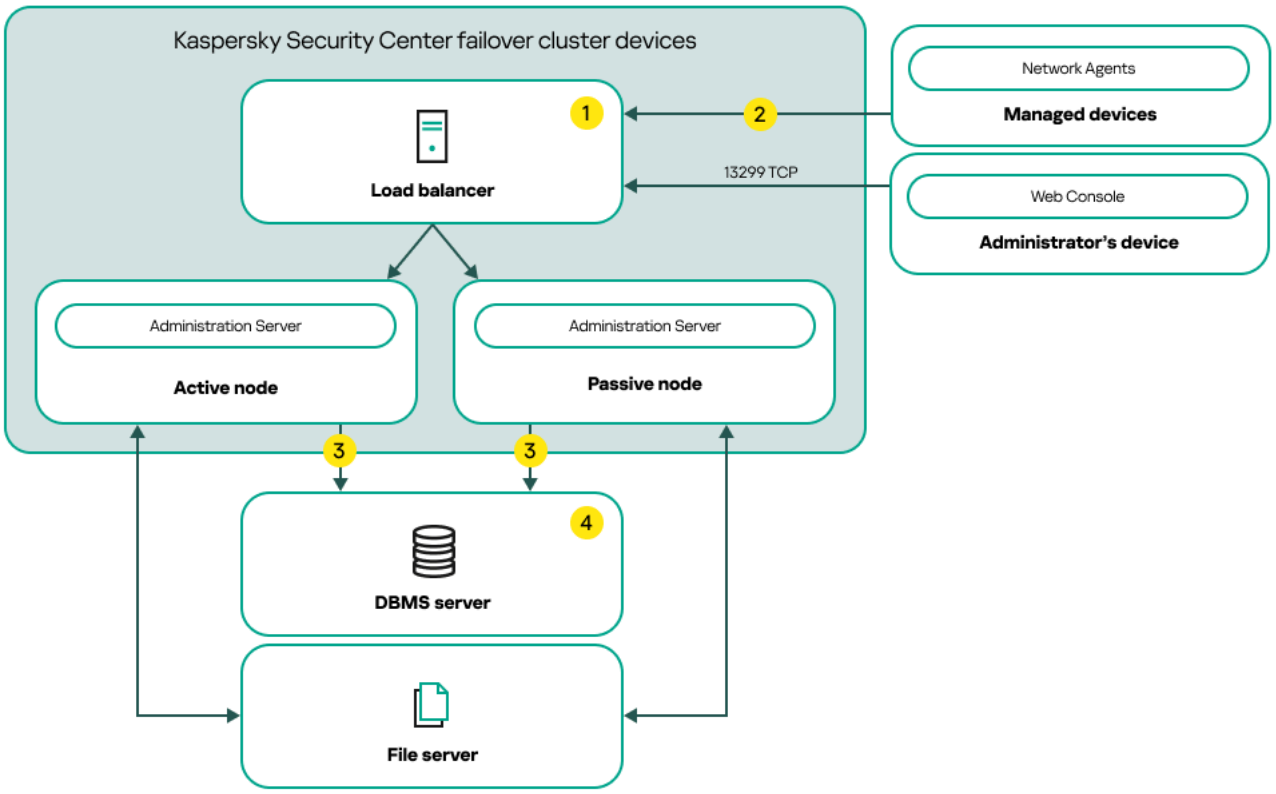
Scheme legend:

1 Administration Server sends data to the database. Open the necessary ports on the device where the database is located, for example, port 3306 for MySQL Server, or port 5432 for PostgreSQL or Postgres Pro. Please refer to the DBMS documentation for the relevant information.

2 Open the following ports on devices with the Administration Server to connect to managed devices: TCP 13000, UDP 13000, and TCP 17000.

3 A device with Database Management System (DBMS). If you use MariaDB Galera Cluster as a DBMS, a dedicated device for this purpose is not required. Install MariaDB Galera Cluster on each of the nodes.

A scheme that uses a third-party load balancer and a DBMS installed on a dedicated device




A scheme that uses a third-party load balancer and a DBMS installed on a dedicated device

Scheme legend:

1 On the load balancer device, open all of the Administration Server ports: TCP 13000, UDP 13000, TCP 13299, and TCP 17000.

> If you want to use the klakaut utility for automation, you must also open the TCP 13291 port.

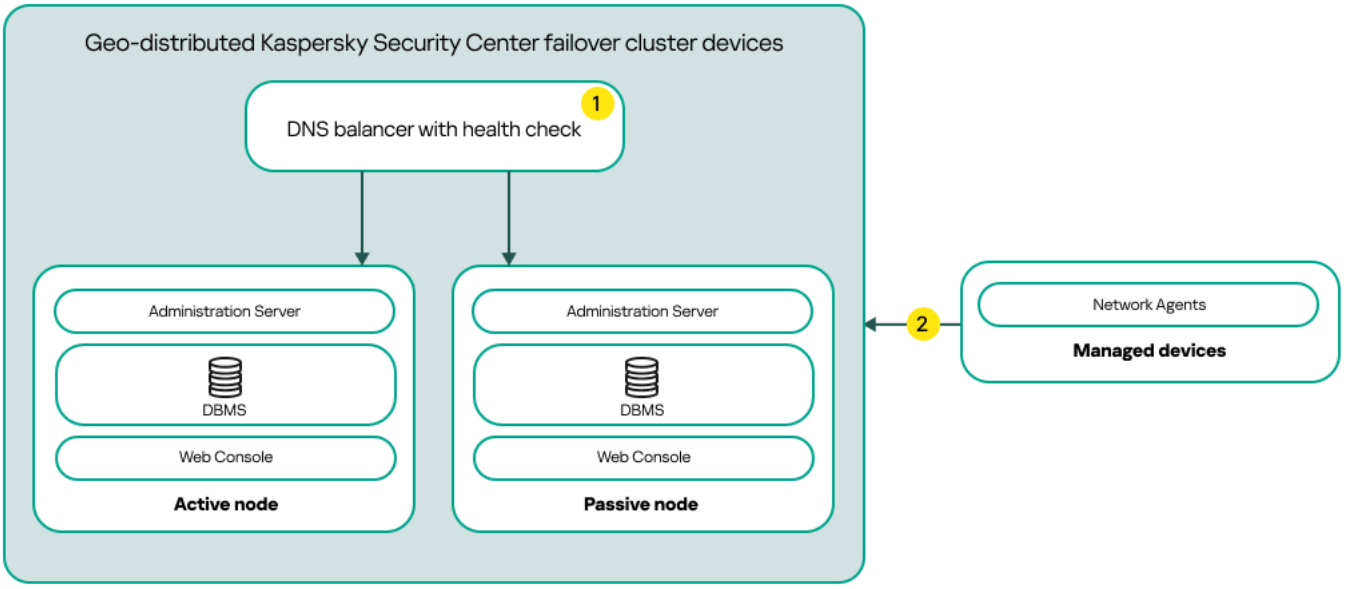
2 Open the following ports on devices with the Administration Server to connect to managed devices: TCP 13000, UDP 13000, and TCP 17000.

3 Administration Server sends data to the database. Open the necessary ports on the device where the database is located, for example, port 3306 for MySQL Server, or port 5432 for PostgreSQL or Postgres Pro. Please refer to the DBMS documentation for the relevant information.

4 A device with Database Management System (DBMS). If you use MariaDB Galera Cluster as a DBMS, a dedicated device for this purpose is not required. Install MariaDB Galera Cluster on each of the nodes.

Geo-distributed Kaspersky Security Center Linux failover cluster

This deployment scheme allows you to provide high availability of all components. In this scheme, Administration Server, DBMS, and Kaspersky Security Center Web Console are installed on the both cluster nodes.




Deployment scheme of the geo-distributed Kaspersky Security Center Linux failover cluster

1 DNS balancer with health check that must be deployed on your side before the geo-distributed Kaspersky Security Center Linux failover cluster installation.

DNS balancer periodically checks the status of the cluster nodes. When accessing the cluster by its domain name, the DNS balancer always returns the IP address of the active node.

2 Open the following ports on devices with the Administration Server to connect to managed devices: TCP 13000, UDP 13000, and TCP 17000.

# Kaspersky Security Center Linux failover cluster

This section contains general information about the Kaspersky Security Center Linux failover cluster deployed within a single data center, as well as instructions for preparing and deploying of the Kaspersky Security Center Linux failover cluster in your network.

## Scenario: Deployment of Kaspersky Security Center Linux failover cluster

A Kaspersky Security Center Linux failover cluster provides high availability of Kaspersky Security Center Linux and minimizes downtime of Administration Server in case of a failure. The failover cluster is based on two identical instances of Kaspersky Security Center Linux installed on two computers. One of the instances works as an active node and the other one is a passive node. The active node manages protection of the client devices, while the passive one is prepared to take all of the functions of the active node in case the active node fails. When a failure occurs, the passive node becomes active and the active node becomes passive.

Kaspersky applications deployment proceeds in stages:

It is recommended to follow the sequence of stages described in this scenario.

1. **Checking the hardware requirements**

   Ensure that you have the hardware that meets the requirements for the failover cluster.

2. **Choosing the deployment schema**

   Choose the deployment schema. This affects the next stages of deployment.

3. **Preparing user accounts for Kaspersky Security Center Linux services**

   Perform the following steps on the active node, passive node and file server:

   1. Create a `kladmins` group. Run the following commands:

      `sudo groupadd kladmins`

      `sudo groupmod -g <new_GID> kladmins`

      Ensure that the group has the same GID on all three devices. Execute the following command:

      `getent group kladmins`

      If GID do not match, you can use the following command to specify GID:

      `sudo groupmod -g <new_GID> kladmins`

   2. Create a `ksc` user account. Assign user accounts to the `kladmins` group. Run the following commands:

      `sudo adduser ksc`

      `sudo usermod -u <new_UID> ksc`

      `sudo gpasswd -a ksc kladmins`

      `sudo usermod -g kladmins ksc`

      Ensure that the user account has the same UID on all three devices. Execute the following command:

      `getent passwd ksc`

      If UID do not match, you can use the following command to specify UID:

      `sudo usermod -u <new_UID> ksc`

   3. Create a `rightless` user account. Assign user accounts to the `kladmins` group. Run the following commands:

      `sudo adduser rightless`

      `sudo usermod -u <new_UID> rightless`

      `sudo gpasswd -a rightless kladmins`

      `sudo usermod -g kladmins rightless`

      Ensure that the user account has the same UID on all three devices. Execute the following command:

      `getent passwd rightless`

      If UID do not match, you can use the following command to specify UID:

      `sudo usermod -u <new_UID> rightless`

4. Create a `ksciam` user account. Assign user accounts to the `kladmins` group. Run the following commands:

   ```
   sudo adduser ksciam
   ```

   ```
   sudo usermod -u <new_UID> ksciam
   ```

   ```
   sudo gpasswd -a ksciam kladmins
   ```

   ```
   sudo usermod -g kladmins ksciam
   ```

   Ensure that the user account has the same UID on all three devices. Execute the following command:

   ```
   getent passwd ksciam
   ```

   If UID do not match, you can use the following command to specify UID:

   ```
   sudo usermod -u <new_UID> ksciam
   ```

5. If necessary, increase the default limit of files that can be opened (file descriptors) for the accounts used for the function of Kaspersky Security Center Linux services. To do this, open the /etc/security/limits.conf file, and then specify the soft and hard limits of the file descriptors as follows:

   ```
   ksc soft nofile <max_number_of_opened_files>
   ```

   ```
   ksc hard nofile <max_number_of_opened_files>
   ```

   By default, limits of the file descriptors are specified during the installation. The soft file limit is 32 768 files, the hard file limit is 131 072 files.

**4 File server preparation**

Prepare the file server to work as a component of Kaspersky Security Center Linux failover cluster. Make sure that the file server meets the hardware and software requirements, create two shared folders for Kaspersky Security Center Linux data, and configure permissions to access the shared folders.

How-to instructions: Preparing a file server for Kaspersky Security Center Linux failover cluster

**5 DBMS installation**

Install the DBMS for Kaspersky Security Center Linux. You can choose one of supported DBMS. For information about how to install the selected DBMS, refer to its documentation.

If the distribution of your Linux-based operating system does not contain a supported DBMS, you can install the DBMS from a third-party package repository.

After installing the DBMS, follow the corresponding instruction:

- Configuring the PostgreSQL or Postgres Pro server for working with Kaspersky Security Center Linux
- Configuring the MariaDB x64 server for working with Kaspersky Security Center Linux

Manually create a database for IAM. The Administration Server does not remove the IAM database automatically when uninstalling or moving the server to another device, you must remove the database manually.

- For PostgreSQL, run the following command:

  ```
  sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
  ```

- For MariaDB, run the following command:

  ```
  sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
  ```

On the device with the DBMS installed, configure connection to devices that will work as an active and passive nodes.

6. **Preparation of active and passive nodes**

   Prepare two devices with identical hardware and software to work as an active and passive nodes.

   How-to instructions: Preparing nodes for Kaspersky Security Center Linux failover cluster

7. **Installing Kaspersky Security Center Linux**

   Install Kaspersky Security Center Linux in the failover cluster mode on both nodes.

   You must first install Kaspersky Security Center Linux on the device that you want to be the active node, and then install it on the passive one.

   How-to instructions: Installing Kaspersky Security Center Linux on the Kaspersky Security Center Linux failover cluster nodes.

8. **Installing Kaspersky Security Center Web Console**

   Install Kaspersky Security Center Web Console on a separate device that is not a cluster node.

   Specify the failover cluster as the Administration server address in the answer file.

   The Administration server certificate is located at the following path:
   /mnt/KlFocDataShare_klfoc/1093/cert/klserver.cer

   Copy the certificate file to the device on which Kaspersky Security Center Web Console is being installed. Specify the local path to the certificate in the answer file.

9. **Testing the failover cluster**

   Check that you configured the failover cluster correctly and it works properly. For example, you can run the following command to initiate switching to the passive node:

   `/opt/kaspersky/ksc64/sbin/klfoc -failover --stp klfoc`

   Use the following command to verify that failover cluster management service is `Active: active (running)` on both nodes:

   `systemctl status klfocsvc_klfoc`

   Use the following commands to verify that other failover cluster services are `Active: active (running)` on the active node. On the passive node, these failover cluster services must be `Active: inactive (dead)` or `Active: failed (Result: signal)`.

   - `systemctl status klnagent_klfoc`
   - `systemctl status kladminserver_klfoc`
   - `systemctl status klactprx_klfoc`
   - `systemctl status klwebsrv_klfoc`

Kaspersky Security Center Linux failover cluster is deployed.

# Kaspersky Security Center Linux failover cluster. Hardware and software requirements

We recommend that after installing Administration Server on a device, you install Kaspersky Endpoint Security for Linux on this device.
For the concurrent installation, you must have minimum 300 IOPS as well as add to the Administration Server requirements 1,5 GB of RAM, and 15% to the CPU.
For hardware requirements of Kaspersky Endpoint Security, refer to the Kaspersky Endpoint Security for Linux Help.

For information about the security settings required to work with Kaspersky Security Center Linux, refer to the Kaspersky Endpoint Security for Linux Help.

To deploy a Kaspersky Security Center Linux failover cluster, you must have the following hardware:

- Two devices with identical hardware and software. These devices will act as the active and passive nodes.

  Minimum configuration for active and passive nodes

  | Hardware | Value |
  |---|---|
  | CPU | 2 cores, 2500 MHz |
  | RAM | 6 GB |
  | Disk space | 10 GB, 150 IOPS or higher |
  | Network interface controller | 1 Gbps |

  Failover cluster deployment fails when you have either both arping and iputils-arping packages or only the arping package installed. Before deploying a failover cluster, ensure that you only have the iputils-arping package installed on both nodes.

  You can review the sizing requirements for active and passive nodes depending on the number of managed devices in the Hardware requirements for the DBMS and the Administration Server article.

- A device on which you want to install the Kaspersky Security Center Linux Web Console.

  Device configuration for 10 or fewer system administrators

  | Hardware | Value |
  |---|---|
  | CPU | 2 cores, 2500 MHz |
  | RAM | 4 GB |
  | Disk space | 40 GB, 150 IOPS or higher |

  Device configuration for more than 10 system administrators

  | Hardware | Value |
  |---|---|
  | CPU | 4 cores, 2500 MHz |
  | RAM | 8 GB |
  | Disk space | 40 GB, 150 IOPS or higher |

- A file server that supports the CIFS/SMB protocol, version 2.0 or later. You must provide a dedicated device that will act as a file server.

  Configuration of a file server

  | Hardware | Value |
  |---|---|
  | CPU | 4 cores, 2500 MHz |
  | RAM | 32 GB |
  | Disk space | 500 GB, 500 IOPS or higher |
  | Network interface controller | 10 Gbps |

  Make sure you have provided high network bandwidth between the file server, and the active and passive nodes.

- A device with Database Management System (DBMS). If you use MariaDB Galera Cluster as a DBMS, a dedicated device for this purpose is not required.

- A load balancer device. Used in a Kaspersky Security Center Linux failover cluster deployment scheme involving the use of a third-party load balancer and the DBMS installed on a dedicated device.

  Device configuration for a Nginx load balancer

  | Hardware | Value |
  |---|---|
  | CPU | 2 cores, 2500 MHz |
  | RAM | 4 GB |

## Preparing a file server for a Kaspersky Security Center Linux failover cluster

A file server works as a required component of a Kaspersky Security Center Linux failover cluster.

*To prepare a file server:*

1. Make sure that the file server meets the hardware and software requirements.

2. Install and configure an NFS server:

   - Access to the file server must be enabled for both nodes in the NFS server settings.

   - The NFS protocol must have version 4.0 or 4.1.

   - Minimum requirements for Linux kernel:

     - 3.19.0-25, if you use NFS 4.0

     - 4.4.0-176, if you use NFS 4.1

   Depending on your Linux distribution, install either nfs-utils package or nfs-kernel-server package by running the corresponding command:

   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

3. On the file server, create two folders and share them by using NFS. One of them is used to keep information about the failover cluster state. The other one is used to store the data and settings of Kaspersky Security Center Linux. You will specify paths to the shared folders while configuring the installation of Kaspersky Security Center Linux.

   Ensure that the following folders do not exist:

   - `/mnt/KlFocStateShare`
   - `/mnt/KlFocDataShare_klfoc`

   If any of these folders exists, recursively delete it.

   Run the following commands:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 770 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo systemctl start nfs-server
   ```

   Enable autostart by running the following command:

   ```
   sudo systemctl enable rpcbind
   ```

   You can specify custom folders, but we recommend that you use the suggested folder names for convenience when using the Help.

4. Restart the file server.

The file server is prepared. To deploy the Kaspersky Security Center Linux failover cluster, follow the further instructions in this scenario.

## Preparing nodes for a Kaspersky Security Center Linux failover cluster

Before continuing, ensure that you completed the previous steps in the Scenario: Deployment of Kaspersky failover cluster.

Prepare two devices to work as the active and passive nodes of the Kaspersky Security Center Linux failover cluster.

### Common folders configuration

*To configure common folders:*

1. Depending on your Linux distribution, install either nfs-utils package or nfs-kernel-server package on each node by running the corresponding command:

   ```
   yum install nfs-utils
   ```

`apt install nfs-kernel-server`

2. Create mount points by running the following commands:

   `mkdir -p /mnt/KlFocStateShare`

   `mkdir -p /mnt/KlFocDataShare_klfoc`

3. Match the mount points and the shared folders:

   `sudo sh -c "echo <file server>:/mnt/KlFocStateShare /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"`

   `sudo sh -c "echo <file server>:/mnt/KlFocDataShare_klfoc /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"`

   Where, `{file server}` is the FQDN of the file server with shared folders.

4. Mount the shared folders by running the following commands:

   `mount /mnt/KlFocStateShare`

   `mount /mnt/KlFocDataShare_klfoc`

5. Ensure that the permissions to access the shared folders belong to ksc:kladmins.

   Execute the following command:

   `ls -la /mnt/`

Network adapters configuration

A secondary network adapter can be physical or virtual. If you chose a deployment schema with a secondary network adapter, perform the corresponding procedure on both nodes:

- Use a virtual secondary network adapter based on a physical network adapter (the MACVLAN technology):

  1. Install the iputils-arping package. Depending on your Linux distribution, run one of the following commands:

     - `yum install iputils`

     or

     - `apt install iputils-arping`

  2. To ensure that NetworkManager is used to manage the physical network adapter, run the following command:

     `nmcli device status`

     If the command output shows the physical network adapter as not being managed, configure the NetworkManager to manage the physical network adapter. The exact configuration steps depend on your Linux distributive.

  3. To identify interfaces, use the following command:

     `ip a`

  4. To create a configuration profile, run the following command:

     `nmcli connection add type macvlan dev <physical interface> mode bridge ifname <virtual interface> ipv4.addresses <address mask> ipv4.method manual autoconnect no`

- Use a physical secondary network adapter or create a virtual TAP device using a hypervisor. In this scenario, disable the NetworkManager software.

  1. Connect the secondary network adapter to a node.

  2. Install the iputils-arping package. Depending on your Linux distribution, run one of the following commands:

     - `yum install iputils`

     or

     - `apt install iputils-arping`

  3. To delete the NetworkManager connection for the target interface, run the following command:

     `nmcli con del <connection name>`

     To check connections to the target interface, run the following command:

     `nmcli con show`

  4. Modify the NetworkManager.conf file. Locate the key file section and assign the target interface to the `unmanaged-devices` parameter:

     `[keyfile]`

     `unmanaged-devices=interface-name:<interface name>`

  5. Restart the NetworkManager:

     `systemctl reload NetworkManager`

     To ensure that the target interface is no longer managed, run the following command:

     `nmcli dev status`

Load balancer configuration

If you chose a deployment schema with a load balancer, follow the instruction below to configure it.

*To configure the load balancer:*

1. Prepare a dedicated Linux-based device with nginx or another load balancer installed.

2. Configure load balancing. Set the active node as the main server, and the passive node as a backup server.

3. On the nginx server, open all of the Administration Server ports according to the following article: Ports used by Kaspersky Security Center Linux.

To deploy Kaspersky Security Center Linux failover cluster, follow the further instructions of the scenario.

> The availability of the failover cluster nodes should be determined by the availability of the main connection ports to the Administration Server. The passive node does not accept any external connections until a switch occurs.

## Installing Kaspersky Security Center Linux on the Kaspersky Security Center Linux failover cluster nodes

Before continuing, ensure that you completed the previous steps in the Scenario: Deployment of Kaspersky failover cluster.

This procedure describes how to install Kaspersky Security Center Linux on the nodes of the Kaspersky Security Center Linux failover cluster. Kaspersky Security Center Linux is installed on both nodes of the Kaspersky Security Center Linux failover cluster separately. First, you install the application on the active node, then on the passive one. When installing, you choose which node will be active and which will be passive.

Depending on the Linux distribution installed on your device, you have to use one of the following installation files:

- ksc64_[version_number]_amd64.deb
- ksc64-[version_number].x86_64.rpm

You receive the installation file by downloading it from the Kaspersky website.

If you use RED OS version 7.3.4 or newer or MSVSPHERE version 9.2 or newer, you have to install the libxcrypt-compat package on both nodes.

Installation on the active node

*To install Kaspersky Security Center Linux on the active node:*

1. Make sure that the device on which you want to install Kaspersky Security Center Linux is running one of the supported Linux distributions.
2. If you use a secondary network adapter, enter its name when prompted. You can enter the following command to display all network interfaces:

   ```
   ip addr
   ```

3. Run the Kaspersky Security Center Linux installation. Depending on your Linux distribution, run one of the following commands:

   - `sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm`

4. Run the Kaspersky Security Center Linux configuration:

   ```
   /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Read the End User License Agreement (EULA) and the Privacy Policy. The text is displayed in the command line window. Press the space bar to view the next text segment. Then, when prompted, enter the following values:

   a. Enter `y` if you understand and accept the terms of the EULA. Enter `n` if you do not accept the terms of the EULA. To use Kaspersky Security Center Linux, you must accept the terms of the EULA.

   b. Enter `y` if you understand and accept the terms of the Privacy Policy, and if you agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. Enter `n` if you do not accept the terms of the Privacy Policy. To use Kaspersky Security Center Linux, you must accept the terms of the Privacy Policy.

6. Select **Primary cluster node** as an Administration Server installation mode.

7. When prompted, specify the following settings:

   a. Enter the local path to the mount point of the state share: `/mnt/KlFocStateShare`

   b. Enter the local path to the mount point of the data share: `/mnt/KlFocDataShare_klfoc`

   c. Choose a failover cluster connectivity mode: through a secondary network adapter or an external load balancer.

   d. If you use a secondary network adapter, enter its name.

   e. Enter the FQDN or DNS name of the secondary network adapter or the FQDN or DNS name of the external load balancer.

   f. Enter the Administration Server SSL port number. The default port number is 13000.

   g. Evaluate the approximate number of devices that you intend to manage:

      - If you have from 1 to 100 managed devices, enter 1.
      - If you have from 101 to 1000 managed devices, enter 2.
      - If you have more than 1000 managed devices, enter 3.

      This setting is used for automatically randomized delay of task starts to optimize network load. The list below shows the interval within which the delay is calculated:

      - 1 to 100 managed devices, value 1. Delay is not used.
      - 101 to 1000 managed devices, value 2. Delay is 5 minutes.
      - More than 1000 managed devices, value 3. Delay is 10 minutes.

   h. Enter the security group name for services. By default, the 'kladmins' group is used.

   i. Enter the account name to start the Administration Server service. The account must be a member of the entered security group. By default, the ksc account is used.

   j. Enter the account name to start other services. The account must be a member of the entered security group. By default, the ksc account is used.

k. Select the DBMS that you installed to work with Kaspersky Security Center Linux:

- If you installed MySQL or MariaDB, enter 1.
- If you installed PostgreSQL or Postgres Pro, enter 2.

l. Enter the DNS name or IP address of the device on which the database is installed.

m. Enter the database port number. This port is used to communicate with Administration Server. By default, the following ports are used:

- Port 3306 for MySQL or MariaDB.
- Port 5432 for PostgreSQL or Postgres Pro.

n. Enter the database name.

o. Enter the login of the database administrator account that you use to access the database.

p. Enter the password of the database administrator account that you use to access the database.

q. Enter the FQDN or DNS name of the IAM server.

Enter the value that you specified at step 7e.

r. Enter the account name to start the IAM service. The account must be a member of the entered security group. By default, the ksciam account is used.

s. Select the DBMS that you installed to work with the IAM service:

- If you installed MySQL or MariaDB, enter 1.
- If you installed PostgreSQL or Postgres Pro, enter 2.

t. Enter the IAM DBMS address to be used by the IAM service.

u. Enter the IAM DBMS port number. This port is used to communicate with the IAM service. By default, the following ports are used:

- Port 3306 for MySQL or MariaDB.
- Port 5432 for PostgreSQL or Postgres Pro.

v. Enter the IAM database name to be used by the IAM service. The name of the database used by IAM service should be different from database used by the Administration Server.

w. Enter the login of the database account that you use to access the IAM database.

x. Enter the password of the database account that you use to access the IAM database.

8. Wait for the services to be added and started automatically:

- klfocsvc_klfoc
- kladminserver_klfoc

- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc
- kliam_klfoc

9. Create an account that will act as an Administration Server administrator. Enter the user name and password. The user password cannot have fewer than 8 or more than 256 characters.

   If you skip this step, you can create the account later by running the following command:

   `/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>`

The user is added and Kaspersky Security Center Linux is installed on the primary node.

Installation on the secondary (passive) node

*To install Kaspersky Security Center Linux on the secondary node:*

1. Make sure that the device on which you want to install Kaspersky Security Center Linux is running one of the supported Linux distributions.
2. Run the Kaspersky Security Center Linux installation. Depending on your Linux distribution, run one of the following commands:
   - `sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm`
3. Run the Kaspersky Security Center Linux configuration:

   `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`
4. Read the End User License Agreement (EULA) and the Privacy Policy. The text is displayed in the command line window. Press the space bar to view the next text segment. Then, when prompted, enter the following values:
   a. Enter `y` if you understand and accept the terms of the EULA. Enter `n` if you do not accept the terms of the EULA. To use Kaspersky Security Center Linux, you must accept the terms of the EULA.
   b. Enter `y` if you understand and accept the terms of the Privacy Policy, and if you agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. Enter `n` if you do not accept the terms of the Privacy Policy. To use Kaspersky Security Center Linux, you must accept the terms of the Privacy Policy.
5. Select **Secondary cluster node** as an Administration Server installation mode.
6. When prompted, enter the local path to the mount point of the state share: `/mnt/KlFocStateShare`

Kaspersky Security Center Linux is installed on the secondary node.

Service verification

Use the following command to verify that failover cluster management service is in status `Active: active (running)`:

```
systemctl status klfocsvc_klfoc
```

Use the following commands to verify that other failover cluster services are in status `Active: inactive (dead)`:

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`
- `systemctl status kliam_klfoc`

Now, you can test the Kaspersky Security Center Linux failover cluster to make sure that you configured it correctly and that the cluster works properly.

## Starting and stopping cluster nodes manually

You may need to stop the entire Kaspersky Security Center Linux failover cluster or temporarily detach one of the nodes of the cluster for maintenance. If this is the case, follow the instructions in this section. Do not try to start or stop the services or processes related to the failover cluster by using any other means. This may cause data loss.

Starting and stopping the entire failover cluster for maintenance

*To start or stop the entire failover cluster:*

On the active node, run one of the following commands:

- To stop the cluster, run: `/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- To start the cluster, run: `/opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc`

The failover cluster is started or stopped, depending on the command that you run.

Maintaining one of the nodes

*To maintain one of the nodes:*

1. On the active node, stop the failover cluster by using the `klfoc -stopcluster --stp klfoc` command.
2. On the node that you want to maintain, go to /opt/kaspersky/ksc64/sbin.
3. Open command line, and then detach the node from the cluster by running the `detach_node.sh` command.
4. On the active node, start the failover cluster by using the `klfoc -startcluster --stp klfoc` command.
5. Perform maintenance activities.
6. On the active node, stop the failover cluster by using the `klfoc -stopcluster --stp klfoc` command.

7. On the node that was maintained, go to /opt/kaspersky/ksc64/sbin.
8. Open command line, and then attach the node to the cluster by running the `attach_node.sh` command.
9. On the active node, start the failover cluster by using the `klfoc -startcluster --stp klfoc` command.
10. To ensure that the current node is active, run the following commands to check if the services are run:

    `systemctl status klnagent_klfoc.service`

    `systemctl status kladminserver_klfoc.service`

    `systemctl status klactprx_klfoc.service`

    `systemctl status klwebsrv_klfoc.service`

    `systemctl status kliam_klfoc.service`

    These services are run on the active node and not on the passive node.

The node is maintained and attached to the failover cluster.

## Reinstalling a failover cluster node

*To reinstall a failover cluster node:*

1. Create a backup of the Administration Server.
2. Switch the active node to maintenance mode.
3. If it is necessary to keep the current operating system, perform the following steps.

   If you want to replace the device or operating system, skip this step.

   a. To stop the failover cluster, run the following command:

   `klfoc -stopcluster --stp klfoc`

   b. To forcefully stop failover cluster services, run the following commands:

   `sudo systemctl stop klfocsvc_klfoc`

   `systemctl status kl*klfoc*`

   c. To unmount failover cluster directories, run the following commands:

   `sudo umount /mnt/KlFocDataShare_klfoc`

   `sudo umount /mnt/KlFocStateShare`

   d. To uninstall Kaspersky Security Center Linux, run either of the following commands depending on your Linux distributive:

   - `sudo dpkg --remove ksc64`

   or

   - `sudo yum remove ksc64`

e. Perform all steps from the following instructions for the passive node:

1. Preparing nodes for a Kaspersky Security Center Linux failover cluster.

2. Installing Kaspersky Security Center Linux on the Kaspersky Security Center Linux failover cluster nodes.

4. Exit the maintenance mode. Continue from the step 6 (stopping the failover cluster) of the Starting and stopping cluster nodes manually instruction.

## Installing Kaspersky Security Center Web Console connected to Administration Server installed on Kaspersky Security Center Linux failover cluster nodes

This section describes how to install Kaspersky Security Center Web Console Server (hereinafter also referred to as Kaspersky Security Center Web Console), that connects to Administration Server installed on Kaspersky Security Center Linux failover cluster nodes. Prior to installing Kaspersky Security Center Web Console, install a DBMS and Kaspersky Security Center Linux Administration Server on Kaspersky Security Center Linux failover cluster nodes.

Kaspersky Security Center Web Console does not support installation on cluster nodes. We recommend installing Kaspersky Security Center Web Console on a separate server.

*To install Kaspersky Security Center Web Console that connects to Administration Server installed on Kaspersky Security Center Linux failover cluster nodes:*

1. Perform step 1 and step 2 of the Kaspersky Security Center Web Console installation.

2. At step 3, in the response file, specify the `trusted` installation parameter to allow the Kaspersky Security Center Web Console to connect to Kaspersky Security Center Linux failover cluster.

   **Components of the trusted installation parameter**

   If you connect to the Kaspersky Security Center Linux failover cluster by using domain authentication with SSO, specify the trusted installation parameter as follows: If you connect Kaspersky Security Center Web Console to Administration Server version 16 or later, domain authentication with single sign-on (SSO) provided by Identity and Access Manager (IAM) will be used. In this case, specify the `trusted` installation parameter as follows:

```
"trusted":  {
  "<Administration Server name>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<shared data folder>/iam/main_certificate.pem",
    "iamPATPath": "<shared data folder>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<shared data folder>/1093/cert/klserver.cer"
  }
}
```

where:

- `< Administration Server name >` is the Kaspersky Security Center Linux failover cluster name that will be displayed in the login window of Kaspersky Security Center Web Console.

- `iamHost` is the address of the device where Administration Server and IAM are installed. If you created a secondary network adapter when preparing the cluster nodes, use the FQDN or host name of the adapter as the Kaspersky Security Center Linux failover cluster address. Otherwise, specify the FQDN or host name of the third-party load balancer that you use.

  The `iamHost` value must match the IAM address specified when installing the Administration Server. To obtain the specified IAM address, run the following command on the device with Administration Server installed:

  `grep "iam_address:" <shared data folder>/iam/iam_config.yaml`

- `iamOAuthPort` is the port that is used for exchanging authentication tokens over the OpenID Connect authentication protocol (default value is 4444). This port is used both for communication between Kaspersky Security Center Web Console Server and Administration Server, and between the browser (used with Kaspersky Security Center Web Console) and Administration Server.

- `iamProxyPort` is the port that is used for connecting Kaspersky Security Center Web Console Server to Administration Server (default value is 9050).

- `iamCertPath` is the path to the IAM certificate. The IAM certificate is created automatically the first time you run Administration Server. The certificate is located on the device where Administration Server is installed. The default path to the certificate is: `< shared data folder >/iam/main_certificate.pem`. The certificate is located in the shared data storage of the Kaspersky Security Center Linux failover cluster. The self-signed IAM certificate is rotated automatically.

- `iamPATPath` is the path to the token used for registration of Kaspersky Security Center Web Console as an OAuth-client in IAM. This file is generated automatically the first time you run Administration Server. The token is located on the device where Administration Server is installed. The default path to the token is: <shared data folder>/iam/initial_token.txt. The token is located in the shared data storage of the Kaspersky Security Center Linux failover cluster. The token is valid indefinitely and does not require rotation.

- `kscPort` is the OpenAPI port that Kaspersky Security Center Web Console use to connect to Administration Server (default value is 13299).

- `kscCertPath` is the Administration Server certificate that is located in the shared data storage of the Kaspersky Security Center Linux failover cluster. The default path to the certificate file is: `< shared data folder >\1093\cert\klserver.cer`.

  Copy the Administration Server certificate file (specified by `kscCertPath`), the IAM certificate file (specified by `iamCertPath`), and the token file (specified by `iamPATPath`) from the shared data storage to the device where you install Kaspersky Security Center Web Console. Specify the local path to the Administration Server certificate.

If you connect Kaspersky Security Center Web Console to Administration Server version 15.4 or earlier, authentication by specifying the name and password of the domain user or the internal user will be used. In this case, specify the trusted installation parameter as follows:

```
"trusted":  {
  "<Administration Server name>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<shared data folder>/1093/cert/klserver.cer"
```

```
    }
  }
```

where:

- `<Administration Server name>` is the Kaspersky Security Center Linux failover cluster name that will be displayed in the login window of Kaspersky Security Center Web Console.
- `kscHost` is the Administration Server address (FQDN or host name). If you created a secondary network adapter when preparing the cluster nodes, use the address of the adapter as the Kaspersky Security Center Linux failover cluster address. Otherwise, specify the address of the third-party load balancer that you use.
- `kscPort` is the OpenAPI port that Kaspersky Security Center Web Console uses to connect to Administration Server (default value is 13299).
- `kscCertPath` is the Administration Server certificate that is located in the shared data storage of the Kaspersky Security Center Linux failover cluster. The default path to the certificate file is: `<shared data folder>\1093\cert\klserver.cer`. Copy the certificate file from the shared data storage to the device where you install Kaspersky Security Center Web Console. Specify the local path to the Administration Server certificate.

3. Continue with the standard installation of Kaspersky Security Center Web Console.

When the installation is complete, you can use your browser to open and log in to Kaspersky Security Center Web Console.

# Geo-distributed Kaspersky Security Center Linux failover cluster

This section contains general information about the geo-distributed Kaspersky Security Center Linux failover cluster, as well as instructions for preparing and deploying the geo-distributed failover cluster in your network for the following configurations:

- Cluster nodes running Ubuntu with the PostgreSQL DBMS
- Cluster nodes running SberLinux with the Platform V Pangolin DBMS

## Geo-distributed cluster running Ubuntu with PostgreSQL DBMS

Following this scenario, you can prepare your infrastructure and deploy a geo-distributed Kaspersky Security Center Linux failover cluster.

Prerequisites

- Deploy a highly available DNS balancer with health check.
- Make sure that the active and passive cluster nodes are two devices with identical hardware and software configurations.
  - Hardware requirements:
    - CPU — 16 cores, 2500 MHz
    - RAM–32 GB

- Disk space — 500 GB with 300 IOPS or higher
- Network interface controller — 1 Gbps

- Software requirements:
  - Operating system: Ubuntu Server 24.04 LTS (Noble Numbat) 64-bit
  - DBMS: PostgreSQL 17 64-bit

Stages

Kaspersky Security Center Linux failover cluster deployed within a single data center cannot be upgraded to a geo-distributed failover cluster.

Deployment of the geo-distributed Kaspersky Security Center Linux failover cluster proceeds in stages:

1. **Preparing a file system of failover cluster nodes**

   Prepare the file system on both cluster nodes. The preparation includes creating LVM logical volumes and configuring directories as mount points.

2. **Configuring a replicated cluster file system**

   Install DRBD utilities and configure DRBD resources for data replication between failover cluster nodes. After that, create a replicated file system on the active cluster node.

3. **Installing and configuring Corosync and Pacemaker on the failover cluster nodes**

   Install Corosync and Pacemaker to provide cluster communication and resource management for high availability.

4. **Installing and configuring the PostgreSQL DBMS**

   Install and configure PostgreSQL on cluster nodes.

5. **Installing Kaspersky Security Center Linux on the failover cluster nodes**

   Install Kaspersky Security Center Linux on cluster nodes, and then configure encryption between cluster nodes.

6. **Installing Kaspersky Security Center Web Console on the failover cluster nodes**

   Install Kaspersky Security Center Web Console on both failover cluster nodes to provide high availability.

## Preparing a file system of cluster nodes

As the first step in preparing for the deployment of the geo-distributed Kaspersky Security Center Linux failover cluster, you must set up the file system on both cluster nodes. The preparation includes creating LVM logical volumes and configuring directories as mount points. Perform the procedure below on both cluster nodes.

*To prepare a file system of cluster nodes:*

1. Create an LVM logical volume for the Administration Server data and database:

```
lvcreate -L <volume size> -n klfocdata <volume group name>
```

Create a separate LVM logical volume for storing the answer file:

```
lvcreate -L <volume size> -n klfocstate <volume group name>
```

where:

- `volume group name` is the volume group name used by LVM.
- `klfocdata` and `klfocstate` are logical volume names. These logical volumes are created inside the volume group.

  We recommend using these volume names for consistency, although you can specify custom names if needed.
- `volume size` a size of the volume. We recommend allocating at least 500 GB for the Administration Server data and database. The volume for storing the answer file requires a small amount of space.

2. Create directories to be used as mount points for the logical volumes.
   - For the Administration Server data and database:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```
   - For the answer file:

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

We recommend using the `/mnt/KlFocDataShare_klfoc` and `/mnt/KlFocStateShare_klfoc` directories for consistency, although you can specify custom names if needed.

The file system of cluster nodes is prepared. After that, you have to configure a replicated cluster file system.

## Configuring a replicated cluster file system

### Installing and configuring DRBD

*DRBD* is third-party software used for data replication (specifically for the data volumes and mount points prepared in the previous step).

After you prepare the file system of cluster nodes, you must install DRBD utilities and configure DRBD resources for data replication between cluster nodes. Perform the procedure below on both cluster nodes.

*To install and configure DRBD on cluster nodes:*

1. Install DRBD utilities:

   ```
   apt update
   apt install -y drbd-utils
   ```

   We recommend using DRBD version 9.2.6 or later, because it provides built-in traffic encryption.

   DRBD traffic also can be encrypted by using your own VPN solution.

2. Create DRBD resource configuration files for each logical volume created during a file system preparation (`klfocdata` and `klfocstate`).

   All configuration files must be placed in `/etc/drbd.d/`.

   - Resource `klfocdata` (Administration Server data and database)

     Use asynchronous replication (protocol A) for the klfocdata resource. Configure all other parameters according to your environment.

     **Example configuration file:**

```
resource klfocdata {
    protocol A;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

   - Resource `klfocstate` (the answer file)

     Use the synchronous replication (protocol C) to create the klfocstate resource. Configure all other parameters according to your environment.

     **Example configuration file:**

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Initialize DRBD metadata for both resources:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Start DRBD on all configured resources:

```
drbdadm up all
```

DRBD is installed and configured on both cluster nodes.

### Create a replicated file system on the active cluster node

After you install and configure DRBD on both cluster nodes, create a replicated file system on the active cluster node. Perform the procedure below on the active cluster node.

*To create a replicated file system on the active cluster node:*

1. Promote both DRBD resources to the Primary role:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Format the DRBD devices to prepare the replicated volumes for use on the cluster nodes:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Configure file system parameters:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Mount the DRBD devices to the directories created earlier:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

If the multipathd service is installed, it must be configured to ignore devices `/dev/drbd*` on both cluster nodes.

5. Verify the replication status:

```
drbdadm status
```

The output of the correct file system configuration:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

A replicated file system on the active cluster node is configured. After that, you must install and configure Corosync and Pacemaker on the cluster nodes.

## Installing and configuring Corosync and Pacemaker on the cluster nodes

Corosync and Pacemaker provide cluster communication and resource management for high availability. They ensure that services are automatically moved to a healthy node in case of failure, minimizing downtime.

*To install and configure Corosync and Pacemaker on the cluster nodes:*

1. On both cluster nodes, install the required packages:

```
sudo apt install pacemaker -y
sudo apt install crmsh -y
sudo apt install resource-agent-extra -y
```

2. Configure Corosync and Pacemaker on both cluster nodes according to the official documentation. This includes enabling automatic start, generating and distributing the authentication key, and configuring access permissions for the authkey file.

   To ensure the settings are correct, run the following command on one of the cluster nodes:

```
crm status
```

   The expected output should show the cluster status and list all active nodes, confirming that Corosync is running correctly and the nodes are communicating.

3. On both cluster nodes, configure the basic Pacemaker cluster settings:

```
crm configure property stonith-enabled="false"
crm configure property symmetric-cluster="false"
crm configure rsc_defaults resource-stickiness="110"
crm configure rsc_defaults migration-threshold=3
crm configure property no-quorum-policy=ignore
```

4. On both cluster nodes, disable the startup of scripts that will be managed by Corosync:

```
systemctl disable drbd.service
```

5. On one of the cluster nodes, create the DRBD-based resources in Pacemaker.

- DRBD resource for klfocdata

  a. Create a cluster resource for the DRBD volume `klfocdata`, enabling the cluster to manage its state and monitor its health automatically:

  ```
  crm configure primitive drbd_klfocdata ocf:linbit:drbd params drbd_resource="klfocdata" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Create a cluster-managed resource `ms_drbd_klfocdata` based on the created resource `drbd_klfocdata`:

  ```
  crm configure ms ms_drbd_klfocdata drbd_klfocdata meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

  c. Create a mount point for the DRBD volume `fs_klfocdata`, specifying the device, target directory, filesystem type, and mount options:

  ```
  crm configure primitive fs_klfocdata ocf:heartbeat:Filesystem params device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" fstype="ext4" options="data=journal"
  ```

- DRBD resource for klfocstate

  a. Create a cluster resource for the DRBD volume `klfocstate`, enabling the cluster to manage its state and monitor its health automatically:

  ```
  crm configure primitive drbd_klfocstate ocf:linbit:drbd params drbd_resource="klfocstate" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Create a cluster-managed resource ms_drbd_klfocstate based on the created resource `drbd_klfocstate`:

  ```
  crm configure ms ms_drbd_klfocstate drbd_klfocstate meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

  c. Create a mount point for the DRBD volume `fs_klfocstate`, specifying the device, target directory, filesystem type, and mount options:

  ```
  crm configure primitive fs_klfocstate ocf:heartbeat:Filesystem params device="/dev/drbd2" \
  directory="/mnt/KlFocStateShare_klfoc" fstype="ext4" options="noatime"
  ```

6. Set the mount order of the resources where the DRBDs are in the Primary state. Name this resource `cluster_resources`:

```
crm configure colocation cluster_resources inf: fs_klfocdata ms_drbd_klfocdata:Master ms_drbd_klfocstate:Master
```

7. Set up the `group_klfoc` group of resources and services:

```
crm configure group group_klfoc fs_klfocdata fs_klfocstate
```

8. Configure the `group_klfoc` resource group to be started after the corresponding DRBD resources. Name this rule `all_after_drbd`:

```
crm configure order all_after_drbd inf: ms_drbd_klfocdata:promote group_klfoc:start
```

9. Set the preference for starting primary and secondary resources: priority 100 for `node1` and 50 for `node2`:

```
crm configure location loc_klfocdata_one ms_drbd_klfocdata 100: db1 # hostname of the first cluster node
crm configure location loc_klfocdata_two ms_drbd_klfocdata 50: db2 # hostname of the second cluster node
crm configure location loc_klfocstate_one ms_drbd_klfocstate 100: db1 # hostname of the first cluster node
crm configure location loc_klfocstate_two ms_drbd_klfocstate 50: db2 # hostname of the second cluster node
crm configure location loc_group_one group_klfoc 100: db1 # hostname of the first cluster node
crm configure location loc_group_two group_klfoc 50: db2 # hostname of the second cluster node
```

10. On both cluster nodes, disable automatic startup of the DRBD service:

```
systemctl disable drbd.service
```

Corosync and Pacemaker are installed and configured on the cluster nodes. After that, you must install the DBMS and create the Administration Server database and the IAM database.

## Installing and configuring the PostgreSQL DBMS

After you install and configure Corosync and Pacemaker on the cluster nodes, you must install the DBMS on both cluster nodes.

*To install and configure the DBMS:*

1. On both cluster nodes, install PostgreSQL 17 x64 or later.

   For information about how to install the PostgreSQL, refer to its documentation.

2. Make sure that cluster nodes with the DBMS installed do not have DBMS user accounts with the following names:

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. On both cluster nodes, stop the DBMS, and then disable automatic startup of the DBMS service:

```
sudo systemctl stop postgresql
sudo systemctl disable postgresql
```

4. On the active cluster node, copy the DBMS directory to the `/mnt/KlFocDataShare_klfoc/dbms` directory:

```
rsync -av /var/lib/postgresql/17/main/ /mnt/KlFocDataShare_klfoc/dbms
mv /var/lib/postgresql/17/main /var/lib/postgresql/17/main.bk
```

5. On the active cluster node, copy the PostgreSQL configuration files to the `/mnt/KlFocDataShare_klfoc/dbms` directory:

```
sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
sudo cp /etc/postgresql/17/main/pg_ident.conf /mnt/KlFocDataShare_klfoc/dbms
```

6. On both cluster nodes, open the configuration file `/etc/postgresql/17/main/postgresql.conf`, and then set the directory `/mnt/KlFocDataShare_klfoc/dbms` as the database data directory.

   Also, specify the paths to configuration files (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` and `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`), and remove the `include_dir` parameter:

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

7. In the configuration file `/etc/postgresql/17/main/postgresql.conf`, adjust the DBMS configuration to meet Kaspersky Security Center Linux requirements.

8. Create and configure accounts for work with PostgreSQL.

9. Create the PostgreSQL service resource:

```
crm configure primitive klfocsvc_dbms ocf:heartbeat:pgsql \
params pgctl="/usr/lib/postgresql/17/bin/pg_ctl" \
psql="/usr/bin/psql" \
pgdata="/mnt/KlFocDataShare_klfoc/dbms" \
config="/etc/postgresql/17/main/postgresql.conf" \
socketdir="/var/run/postgresql" \
op start timeout=60s \
op stop timeout=60s \
op monitor interval=30s timeout=60s
```

10. Add the PostgreSQL resource to the `group_klfoc` cluster group:

```
crm configure edit group_klfoc
```

11. Add the name of the `klfocsvc_dbms` PostgreSQL resource to the end of the list, for example:

```
group group_klfoc {
...
klfocsvc_dbms
}
```

12. On the active cluster node, on the DBMS server, create a database for IAM. The database name must be different from the database that you installed to work with Kaspersky Security Center Linux. Administration Server does not remove the IAM database automatically when uninstalling or moving the server to another device—you must remove the database manually:

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

The DBMS is installed and configured. The Administration Server database and IAM database are created. After that, you have to install Kaspersky Security Center Linux on cluster nodes.

## Installing Kaspersky Security Center Linux on the geo-distributed failover cluster nodes

Kaspersky Security Center Linux is installed on geo-distributed failover cluster nodes by using an answer file in silent mode, that is, without user participation. The answer file contains a custom set of installation parameters: variables and their respective values.

Prerequisites:

- Perform all preparatory steps:
  - Preparing a file system of cluster nodes
  - Configuring a replicated cluster file system
  - Installing and configuring Corosync and Pacemaker on the cluster nodes
  - Installing and configuring the PostgreSQL DBMS
- Make sure that the cluster nodes run Ubuntu Server 24.04 LTS (Noble Numbat) x64.
- Download the installation file `ksc64_[version_number]_amd64.deb` from the Kaspersky website.

Installation on the active node

*To install Kaspersky Security Center Linux on the active node in silent mode:*

1. Read the End User License Agreement. Follow the steps below only if you understand and accept the terms of the End User License Agreement.
2. Create the group `kladmins`, and the unprivileged accounts `ksc` and `ksciam` that must be members of the `kladmins` group. To do this, sequentially run the following commands under an account with root privileges:

```
adduser ksc
groupadd kladmins
gpasswd -a ksc kladmins
usermod -g kladmins ksc
adduser ksciam
gpasswd -a ksciam kladmins
usermod -g kladmins ksciam
```

3. In the directory `/mnt/KlFocDataShare_klfoc/`, create a directory for Kaspersky Security Center Linux files:

```
mkdir /mnt/KlFocDataShare_klfoc/ksc/
```

4. Create the answers file (in TXT format), and add a list of variables in the VARIABLE_NAME=variable_value format to the answer file. Add each variable on a separate line.

In the list of parameters used for Kaspersky Security Center Linux installation in silent mode, specify the following parameters required for the geo-distributed cluster deployment:

- `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

  Set the value `2` to deploy the geo-distributed cluster.

- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` and `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

  The DNS balancer with health check must be already deployed. The values of these parameters must be identical and set to the FQDN of the DNS balancer.

5. Set the value of the `KLAUTOANSWERS` environment variable in the root or user environment containing the full name of the answer file including the path, for example, with the following command:

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. Start the Kaspersky Security Center Linux installation in silent mode by running the following commands:

   - In the root environment:

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

   - In the user environment:

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

7. Disable automatic startup of the service klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

8. After Kaspersky Security Center Linux is installed, stop the active cluster node.

9. Move all cluster resources to the passive node.

   You can use the command `crm node standby` (and bring it back with `crm node online`).

Installation on the passive node

*To install Kaspersky Security Center Linux on the passive node:*

1. Run the Kaspersky Security Center Linux installation:

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

2. Run the Kaspersky Security Center Linux configuration:

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

3. Read the End User License Agreement (EULA) and the Privacy Policy. The text is displayed in the command line window. Press the space bar to view the next text segment. Then, when prompted, enter the following values:

   - Enter `y` if you understand and accept the terms of the EULA. Enter `n` if you do not accept the terms of the EULA. To use Kaspersky Security Center Linux, you must accept the terms of the EULA.

   - Enter `y` if you understand and accept the terms of the Privacy Policy, and if you agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. Enter n if you do not accept the terms of the Privacy Policy. To use Kaspersky Security Center Linux, you must accept the terms of the Privacy Policy.

4. Select the passive cluster node as an Administration Server installation mode.

5. When prompted, enter the local path to the mount point of the state share: `/mnt/KlFocStateShare_klfoc`.

6. Disable automatic startup of the service klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

7. Create the `klfocsvc_klfoc` service resource:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Add the `klfocsvc_klfoc` resource to the `group_klfoc` group:

```
crm configure edit group_klfoc
```

9. Append `klfocsvc_klfoc` at the end of the group line, for example:

```
group group_klfoc {
...
klfocsvc_klfoc
}
```

10. Verify that all resources are in the started state on the active node.

```
crm status
```

Configuring encryption between cluster nodes

*To configure encryption between cluster nodes,*

If you installed DRBD version 9.2.6 or later during configuring a replicated cluster file system, configure encryption between cluster nodes according to the official DRBD documentation.

Alternatively, you can encrypt the traffic between cluster nodes by using your own VPN solution.

Geo-distributed Kaspersky Security Center Linux failover cluster is installed. After that, you must install Kaspersky Security Center Web Console on both cluster nodes.

## Geo-distributed cluster running SberLinux with Platform V Pangolin DBMS

Following this scenario, you can prepare your infrastructure and deploy a geo-distributed Kaspersky Security Center Linux failover cluster.

### Prerequisites

- Deploy a highly available DNS balancer with health check.
- Make sure that the active and passive cluster nodes are two devices with identical hardware and software configurations.
  - Hardware requirements:
    - CPU — 16 cores, 2500 MHz
    - RAM–32 GB
    - Disk space — 500 GB with 300 IOPS or higher
    - Network interface controller — 1 Gbps
  - Software requirements:
    - Operating system: Platform V SberLinux OS Server (SLO) 9.5.1 64-bit
    - DBMS: Platform V Pangolin 6.5.1 64-bit

### Stages

> Kaspersky Security Center Linux failover cluster deployed within a single data center cannot be upgraded to a geo-distributed failover cluster.

Deployment of the geo-distributed Kaspersky Security Center Linux failover cluster proceeds in stages:

1. **Preparing a file system of failover cluster nodes**

   Prepare the file system on both cluster nodes. The preparation includes creating LVM logical volumes and configuring directories as mount points.

2. **Configuring a replicated cluster file system**

   Install DRBD utilities and configure DRBD resources for data replication between failover cluster nodes. After that, create a replicated file system on the active cluster node.

3. **Installing and configuring Corosync and Pacemaker on the failover cluster nodes**

   Install Corosync and Pacemaker to provide cluster communication and resource management for high availability.

4. **Installing and configuring the Platform V Pangolin DBMS**

   Install and configure Platform V Pangolin on cluster nodes.

5. **Installing Kaspersky Security Center Linux on the failover cluster nodes**

   Install Kaspersky Security Center Linux on cluster nodes, and then configure encryption between cluster nodes.

6. **Installing Kaspersky Security Center Web Console on the failover cluster nodes**

   Install Kaspersky Security Center Web Console on both failover cluster nodes to provide high availability.

## Preparing a file system of cluster nodes

As the first step in preparing for the deployment of the geo-distributed Kaspersky Security Center Linux failover cluster, you must set up the file system on both cluster nodes. The preparation includes creating LVM logical volumes and configuring directories as mount points. Perform the procedure below on both cluster nodes.

*To prepare a file system of cluster nodes:*

1. Create an LVM logical volume for the Administration Server data and database:

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Create a separate LVM logical volume for storing the answer file:

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   where:

   - `volume group name` is the volume group name used by LVM.
   - `klfocdata` and `klfocstate` are logical volume names. These logical volumes are created inside the volume group.

     We recommend using these volume names for consistency, although you can specify custom names if needed.

   - `volume size` a size of the volume. We recommend allocating at least 500 GB for the Administration Server data and database. The volume for storing the answer file requires a small amount of space.

2. Create directories to be used as mount points for the logical volumes.

   - For the Administration Server data and database:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - For the answer file:

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

   We recommend using the `/mnt/KlFocDataShare_klfoc` and `/mnt/KlFocStateShare_klfoc` directories for consistency, although you can specify custom names if needed.

The file system of cluster nodes is prepared. After that, you have to configure a replicated cluster file system.

## Configuring a replicated cluster file system

Installing and configuring DRBD

*DRBD* is third-party software used for data replication (specifically for the data volumes and mount points prepared in the previous step).

After you prepare the file system of cluster nodes, you must install DRBD utilities and configure DRBD resources for data replication between cluster nodes. Perform the procedure below on both cluster nodes.

*To install and configure DRBD on cluster nodes:*

1. Install DRBD utilities as follows:

   a. Enable the EPEL and ELRepo repositories on both nodes:

   ```
   dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   dnf install https://www.elrepo.org/elrepo-release-9.el9.elrepo.noarch.rpm
   ```

   b. Output all available versions of the kmod-drbd9x package and filter the package list built for the el9_6 platform (for example, Platform V SberLinux OS Server (SLO) 9.6 is used):

   ```
   dnf search --showduplicates kmod-drbd9x | grep el9_6
   ```

   c. Install the latest available version from the list on both nodes. Example for Platform V SberLinux OS Server (SLO) 9.6:

   ```
   dnf install kmod-drbd9x-9.2.14-1.el9_6.elrepo.x86_64
   dnf install drbd drbd-utils drbd-udev drbd-pacemaker drbd-selinux
   modprobe drbd
   ```

   If a newer version appears in the future, replace the version string accordingly.

   We recommend using DRBD version 9.2.6 or later, because it provides built-in traffic encryption.

   DRBD traffic also can be encrypted by using your own VPN solution.

2. Create DRBD resource configuration files for each logical volume created during a file system preparation (`klfocdata` and `klfocstate`).

   All configuration files must be placed in `/etc/drbd.d/`.

   - Resource `klfocdata` (Administration Server data and database)

     Use asynchronous replication (protocol A) for the klfocdata resource. Configure all other parameters according to your environment.

     **Example configuration file:**

     ```
     resource klfocdata {
         protocol A;
         net {
             after-sb-0pri    discard-least-changes;
             after-sb-1pri    call-pri-lost-after-sb;
             after-sb-2pri    call-pri-lost-after-sb;
         }
         syncer {
             rate 110M;
         }
         # Hostname of the active node
         on db1 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
     ```

```
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

- Resource `klfocstate` (the answer file)

  Use the synchronous replication (protocol C) to create the klfocstate resource. Configure all other parameters according to your environment.

  **Example configuration file:**

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Initialize DRBD metadata for both resources:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. Start DRBD on all configured resources:

```
drbdadm up all
```

DRBD is installed and configured on both cluster nodes.

### Create a replicated file system on the active cluster node

After you install and configure DRBD on both cluster nodes, create a replicated file system on the active cluster node. Perform the procedure below on the active cluster node.

*To create a replicated file system on the active cluster node:*

1. Promote both DRBD resources to the Primary role:

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Format the DRBD devices to prepare the replicated volumes for use on the cluster nodes:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Configure file system parameters:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Mount the DRBD devices to the directories created earlier:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

   If the multipathd service is installed, it must be configured to ignore devices `/dev/drbd*` on both cluster nodes.

5. Verify the replication status:

```
drbdadm status
```

   The output of the correct file system configuration:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

A replicated file system on the active cluster node is configured. After that, you must install and configure Corosync and Pacemaker on the cluster nodes.

## Installing and configuring Corosync and Pacemaker on the cluster nodes

Corosync and Pacemaker provide cluster communication and resource management for high availability. They ensure that services are automatically moved to a healthy node in case of failure, minimizing downtime.

*To install and configure Corosync and Pacemaker on the cluster nodes:*

1. On both cluster nodes, install the required packages:

```
dnf install pcs
dnf install drbd-pacemaker
```

2. Configure Corosync and Pacemaker on both cluster nodes according to the official documentation. This includes enabling automatic start, generating and distributing the authentication key, and configuring access permissions for the authkey file.

   To ensure the settings are correct, run the following command on one of the cluster nodes:

   ```
   pcs status
   ```

   The expected output should show the cluster status and list all active nodes, confirming that Corosync is running correctly and the nodes are communicating.

3. On both cluster nodes, configure the basic Pacemaker cluster settings:

   ```
   pcs property set stonith-enabled=false
   pcs property set symmetric-cluster=false
   pcs resource defaults resource-stickiness=110
   pcs resource defaults migration-threshold=3
   pcs property set no-quorum-policy=ignore
   ```

4. On both cluster nodes, disable the startup of scripts that will be managed by Corosync:

   ```
   systemctl disable drbd.service
   ```

5. On one of the cluster nodes, create the DRBD-based resources in Pacemaker.

   - DRBD resource for klfocdata

     a. Create a cluster resource for the DRBD volume `klfocdata`, enabling the cluster to manage its state and monitor its health automatically:

     ```
     pcs resource create drbd_klfocdata ocf:linbit:drbd \
     drbd_resource="klfocdata" \
     op monitor interval=60s \
     op start interval=0 timeout=240s \
     op stop interval=0 timeout=240s \
     op monitor role=Master interval=10s \
     op monitor role=Slave interval=30s \
     ```

     b. Create a cluster-managed resource `ms_drbd_klfocdata` based on the created resource `drbd_klfocdata`:

     ```
     pcs resource clone drbd_klfocdata promotable=true
     master-max=1
     clone-max=2
     clone-node-max=1 notify=true
     ```

     c. Create a mount point for the DRBD volume `fs_klfocdata`, specifying the device, target directory, filesystem type, and mount options:

     ```
     pcs resource create fs_klfocdata ocf:heartbeat:Filesystem \
     device="/dev/drbd0" \
     directory="/mnt/KlFocDataShare_klfoc" \
     fstype="ext4" \
     options="data=journal"
     ```

- DRBD resource for klfocstate

  a. Create a cluster resource for the DRBD volume `klfocstate`, enabling the cluster to manage its state and monitor its health automatically:

  ```
  pcs resource create drbd_klfocstate ocf:linbit:drbd \
  drbd_resource=klfocstate \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Promoted interval=10s \
  op monitor role=Unpromoted interval=30s \
  ```

  b. Create a cluster-managed resource ms_drbd_klfocstate based on the created resource `drbd_klfocstate`:

  ```
  pcs resource clone drbd_klfocstate promotable=true \
  master-max=1 \
  clone-max=2 \
  clone-node-max=1 \
  notify=true
  ```

  c. Create a mount point for the DRBD volume `fs_klfocstate`, specifying the device, target directory, filesystem type, and mount options:

  ```
  pcs resource create fs_klfocstate ocf:heartbeat:Filesystem \
  device="/dev/drbd2" \
  directory="/mnt/KlFocStateShare_klfoc" \
  fstype="ext4" \
  options="noatime"
  ```

6. On both cluster nodes, disable automatic startup of the DRBD service:

   ```
   systemctl disable drbd.service
   ```

Corosync and Pacemaker are installed and configured on the cluster nodes. After that, you must install the DBMS and create the Administration Server database and the IAM database.

## Installing and configuring the Platform V Pangolin DBMS

After you install and configure Corosync and Pacemaker on the cluster nodes, you must install the DBMS on both cluster nodes.

*To install and configure the DBMS:*

1. On both cluster nodes, install Platform V Pangolin 6.5.1 x64 or later.

   For information about how to install Platform V Pangolin, refer to its documentation.

2. Make sure that cluster nodes with the DBMS installed do not have DBMS user accounts with the following names:

   - client
   - iam
   - ksc

- locker
- pat
- scope
- voltron

3. On the active cluster node, copy the DBMS directory to the `/mnt/KlFocDataShare_klfoc/dbms` directory:

```
sudo rsync -av  /pgdata/06/data/ /mnt/KlFocDataShare_klfoc/dbms
sudo mv /pgdata/06/data/ /pgdata/06/data.bk/
```

4. On both cluster nodes, open the configuration file `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf`, and then set the directory `/mnt/KlFocDataShare_klfoc/dbms` as the database data directory.

   Also, specify the paths to configuration files (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` and `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`), and remove the `include_dir` parameter:

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

5. In the configuration file `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf`, adjust the DBMS configuration to meet Kaspersky Security Center Linux requirements.

6. Create and configure accounts for work with PostgreSQL.

7. Create the DBMS service resource:

```
pcs resource create klfocsvc_dbms pgsql \
pgctl="/usr/pangolin-6.5/bin/pg_ctl"  psql="/usr/bin/psql" pgdata="/mnt/KlFocDataShare_klfoc/dbms"
config="/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf" socketdir="/tmp" \
op start timeout=60s interval=0s \
op stop timeout=60s interval=0s \
op monitor interval=30s timeout=60s \
op promote timeout=120s interval=0s \
op demote timeout=120s interval=0s \
meta target-role=Started
```

8. On both cluster nodes, disable automatic startup of the DBMS service:

```
sudo systemctl disable pangolin.service
```

9. Add the DBMS resource `klfocsvc_dbms` to the `group_klfoc` cluster group:

```
pcs resource group add group_klfoc klfocsvc_dbms
```

10. Append the DBMS resource name `klfocsvc_dbms` at the end of the list, for example:

```
group group_klfoc {
...
klfocsvc_dbms
}
```

11. On the active cluster node, on the DBMS server, create a database for IAM. The database name must be different from the database that you installed to work with Kaspersky Security Center Linux. Administration Server does not remove the IAM database automatically when uninstalling or moving the server to another device—you must remove the database manually:

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

The DBMS is installed and configured. The Administration Server database and IAM database are created. After that, you have to install Kaspersky Security Center Linux on cluster nodes.

## Installing Kaspersky Security Center Linux on the geo-distributed failover cluster nodes

Kaspersky Security Center Linux is installed on geo-distributed failover cluster nodes by using an answer file in silent mode, that is, without user participation. The answer file contains a custom set of installation parameters: variables and their respective values.

Prerequisites:

- Perform all preparatory steps:
  - Preparing a file system of cluster nodes
  - Configuring a replicated cluster file system
  - Installing and configuring Corosync and Pacemaker on the cluster nodes
  - Installing and configuring the Platform V Pangolin DBMS
- Make sure that the cluster nodes run Platform V SberLinux OS Server (SLO) 9.5.1 x64.
- Download the installation file `ksc64_[version_number]_amd64.deb` from the Kaspersky website.

Installation on the active node

*To install Kaspersky Security Center Linux on the active node in silent mode:*

1. Read the End User License Agreement. Follow the steps below only if you understand and accept the terms of the End User License Agreement.
2. Create the group `kladmins`, and the unprivileged accounts `ksc` and `ksciam` that must be members of the `kladmins` group. To do this, sequentially run the following commands under an account with root privileges:

```
adduser ksc
groupadd kladmins
gpasswd -a ksc kladmins
usermod -g kladmins ksc
adduser ksciam
gpasswd -a ksciam kladmins
usermod -g kladmins ksciam
```

3. In the directory `/mnt/KlFocDataShare_klfoc/`, create a directory for Kaspersky Security Center Linux files:

```
mkdir /mnt/KlFocDataShare_klfoc/ksc/
```

4. Create the answers file (in TXT format), and add a list of variables in the VARIABLE_NAME=variable_value format to the answer file. Add each variable on a separate line.

   In the list of parameters used for Kaspersky Security Center Linux installation in silent mode, specify the following parameters required for the geo-distributed cluster deployment:

   - `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

     Set the value `2` to deploy the geo-distributed cluster.

   - `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` and `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

     The DNS balancer with health check must be already deployed. The values of these parameters must be identical and set to the FQDN of the DNS balancer.

5. Set the value of the `KLAUTOANSWERS` environment variable in the root or user environment containing the full name of the answer file including the path, for example, with the following command:

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. Start the Kaspersky Security Center Linux installation in silent mode by running the following commands:

   - In the root environment:

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

   - In the user environment:

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

7. Disable automatic startup of the service klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

8. After Kaspersky Security Center Linux is installed, stop the active cluster node.

9. Move all cluster resources to the passive node.

   You can use the command `pcs node standby` (and bring it back with `pcs node online`).

Installation on the passive node

*To install Kaspersky Security Center Linux on the passive node:*

1. Run the Kaspersky Security Center Linux installation:

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

2. Run the Kaspersky Security Center Linux configuration:

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

3. Read the End User License Agreement (EULA) and the Privacy Policy. The text is displayed in the command line window. Press the space bar to view the next text segment. Then, when prompted, enter the following values:

   - Enter `y` if you understand and accept the terms of the EULA. Enter `n` if you do not accept the terms of the EULA. To use Kaspersky Security Center Linux, you must accept the terms of the EULA.
   - Enter `y` if you understand and accept the terms of the Privacy Policy, and if you agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. Enter n if you do not accept the terms of the Privacy Policy. To use Kaspersky Security Center Linux, you must accept the terms of the Privacy Policy.

4. Select the passive cluster node as an Administration Server installation mode.

5. When prompted, enter the local path to the mount point of the state share: `/mnt/KlFocStateShare_klfoc`.

6. Disable automatic startup of the service klfocsvc_klfoc.service:

```
systemctl disable klfocsvc_klfoc.service
```

7. Create the `klfocsvc_klfoc` service resource:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Add the `klfocsvc_klfoc` resource to the `group_klfoc` group:

```
pcs resource group add group_klfoc klfocsvc_klfoc
```

9. Append `klfocsvc_klfoc` at the end of the group line, for example:

```
group group_klfoc {
...
klfocsvc_klfoc
}
```

10. Verify that all resources are in the started state on the active node.

```
pcs status
```

Configuring encryption between cluster nodes

*To configure encryption between cluster nodes,*

If you installed DRBD version 9.2.6 or later during configuring a replicated cluster file system, configure encryption between cluster nodes according to the official DRBD documentation.

Alternatively, you can encrypt the traffic between cluster nodes by using your own VPN solution.

Geo-distributed Kaspersky Security Center Linux failover cluster is installed. After that, you must install Kaspersky Security Center Web Console on both cluster nodes.

## Installing Kaspersky Security Center Web Console on geo-distributed failover cluster nodes

For a geo-distributed Kaspersky Security Center Linux failover cluster deployment, Kaspersky Security Center Web Console high availability must be supported. To achieve this, Kaspersky Security Center Web Console must be installed on both cluster nodes.

*To install Kaspersky Security Center Web Console:*

1. On both nodes, create a user to work with Kaspersky Security Center Web Console. To do this, run the following command under an account with root privileges:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
   ```

   where the password must contain at least 8 characters.

2. On both nodes, read the End User License Agreement (EULA). If the Kaspersky Security Center Linux distribution kit does not include a TXT file with the text of EULA, you can download the file from the Kaspersky website. If you do not accept the terms of the License Agreement, do not install the application.

3. On both nodes, create a response file that contains parameters for connecting Kaspersky Security Center Web Console to the Administration Server: `/etc/ksc-web-console-setup.json`.

   **Example of a response file containing the minimum set of parameters**

   The set of parameters of the response file depends on the version of the Administration Server to which the Kaspersky Security Center Web Console connects:

   - Administration Server version 16 or later

     Example of a response file with the minimum set of parameters for signing in to Administration Server version 16 or later:

     ```
     {
         "address": "ksc-web-console.example.com",
         "port": 8080,
         "trusted":  {
             "Administration Server v16": {
                 "iamHost": "ksc16.example.com",
                 "iamOAuthPort": 4444,
                 "iamProxyPort": 9050,
                 "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
                 "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
                 "kscPort": 13299,
                 "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
             }
         },
         "certDomain":"ksc-web-console.example.com",
         "acceptEula": true
     }
     ```

- Administration Server version 15.4 or later

  Example of a response file with the minimum set of parameters for signing in to Administration Server version 15.4 or earlier:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

You can install Kaspersky Security Center Web Console either on the same device as Administration Server or on a different device. If Kaspersky Security Center Web Console is installed on a different device, the Kaspersky Security Center Web Console address (specified by `address`) and the Administration Server address (specified by `iamHost` or `kscHost`) differ. If Kaspersky Security Center Web Console is installed on the same device as Administration Server, these parameters have the same values.

The `iamHost` value must match the IAM address that you specified when installing Administration Server. To obtain the specified IAM address, run the following command on the device with Administration Server installed:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

For detailed information, refer to the article: Kaspersky Security Center Web Console installation parameters.

You can add multiple Administration Servers of different versions to the list of trusted servers. In this case, the Servers may use different authentication methods.

We recommend that you specify port numbers above 1024. If you want Kaspersky Security Center Web Console to work on ports below 1024, after installation you have to make sure that you have the setcap utility, and then run the following command:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

If you do not have the setcap utility, you can install it. **Click this link to view the commands.**

For Debian and Ubuntu operating systems, run one of the following commands:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

For SUSE Linux Enterprise Server and Red Hat Enterprise Linux, run the command:

- `sudo zypper install libcap-progs`

4. On both nodes, run the setup file under an account with root privileges.

```
sudo apt-get install ksc-web-console-<build number>.x86_64.deb
```

This starts unpacking of the setup file. Please wait until the installation is complete. Kaspersky Security Center Web Console is installed to the following directory: `/var/opt/kaspersky/ksc-web-console`.

5. On one of the cluster node, create a Pacemaker resource for the KSCWebConsole service to make the KSCWebConsole a Pacemaker-managed service:

```
crm configure primitive ksc_webconsole systemd:KSCWebConsole \
op monitor interval=30s timeout=60s \
op start timeout=120s \
op stop timeout=120s \
meta target-role=Stopped
```

6. On both nodes, stop the KSCWebConsole service and disable its automatic startup:

```
sudo systemctl stop KSCWebConsole
sudo systemctl disable KSCWebConsole
```

7. On one of the cluster nodes, add the `ksc_webconsole` resource to the `group_klfoc` group:

```
crm configure edit group_klfoc
```

8. Append `ksc_webconsole` at the end of the group line, after `klfocsvc_dbms`, for example:

```
group group_klfoc {
...
klfocsvc_dbms
ksc_webconsole
}
```

When the installation is complete, you can use your browser to open and log in to Kaspersky Security Center Web Console.

# Accounts for working with the DBMS

To install and manage the Administration Server and IAM, you need internal database accounts. These accounts allow you to access the database and require certain rights.

A set of the required rights depends on the following criteria:

- DBMS type:
  - MySQL or MariaDB
  - PostgreSQL-based

- Method of the Administration Server database creation:
  - **Automatic**. During the Administration Server installation, you can automatically create an Administration Server database (hereinafter also referred to as a Server database) by using the Administration Server installer (the installer).
  - **Manual**. You can use a third-party application or a script to create an empty database. After that, you can specify this database as the Server database during the Administration Server installation.

The database for the IAM must be created manually, regardless of how you chose to create the Administration Server database.

Follow the principle of least privilege when you grant rights and permissions to the accounts. This means that the granted rights should be only enough to perform the required actions. Do not use standard superuser accounts of your DBMS such as 'root' or 'postgres' as the DBMS connection user for Kaspersky Security Center Linux.

Do not make any manual changes to the Administration Server database and the IAM database, including modifying values, deleting or adding schemas, tables, indexes. Any changes to databases not performed by Administration Server itself disrupt the proper functioning of the Administration Server either immediately or later, for example, after upgrade to the newer version, or while restoring from a backup copy, and so on. Editing of databases is only permitted when you have received explicit instructions from Kaspersky Technical Support.
When uninstalling or migrating the Server to another device, you need to manually delete the databases of the Administration Server and the IAM.

The following information describes the DBMS rights that you need to grant to the accounts before you can install and start the Administration Server.

### MySQL and MariaDB

If you choose MySQL or MariaDB as a DBMS, create a DBMS internal account to access the DBMS, and then grant this account the required rights. Note that the database creation method does not affect the set of rights. The required rights are listed below:

- Schema privileges:
  - Administration Server database: ALL (excluding GRANT OPTION)
  - System schemes (mysql and sys): SELECT, SHOW VIEW
  - The sys.table_exists stored procedure: EXECUTE (if you use MariaDB 10.5 or earlier as a DBMS, you do not need to grant the EXECUTE privilege)
- Global privileges for all schemes: PROCESS, SUPER.

For more information on configuring account rights, see the Creating MySQL and MariaDB databases and user accounts article.

For details on how to move data from a shared tablespace to a file-per-table tablespace, refer to Moving data from shared tablespace to file-per-table tablespace in MySQL and MariaDB DBMSs.

### Configuring privileges for Administration Server data recovery

Rights that you granted to the internal DBMS account are enough to restore Administration Server data from the backup.

### PostgreSQL-based DBMS

Depending on the creation method of the Server database, grant the required rights to the role as described in the table below. For more information on configuring role rights, see the Creating MySQL and MariaDB databases and user accounts article.

Rights of the Postgres role

| Automatic database creation | | Manual database creation |
|---|---|---|
| The *Postgres* user does not require additional rights. | Privileges for a new role: CREATEDB. | For a new role:<br>• Privileges on Administration Server database: ALL.<br>• Privileges on all tables in the public schema: ALL.<br>• Privileges on all sequences in the public schema: ALL. |

### Configuring privileges for Administration Server data recovery

To restore Administration Server data from the backup, the Postgres role used to access to the DBMS must have the owner rights on the Administration Server database.

While you are restoring data from a backup copy, temporarily grant Postgres superuser rights to the standard klserver and kliam accounts that the Administration Server and IAM use to connect to the DBMS (in the example, `klserver` and `kliam` respectively):

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
```

After successful data recovery, restore the original rights of the Postgres user accounts.

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

# Creating MySQL and MariaDB databases and user accounts

Prerequisites

Before creating databases and assigning rights to DBMS user accounts, install and configure one of the servers in accordance with the optimization requirements (if you have not done so earlier):

- MariaDB x64 for working with Kaspersky Security Center Linux
- MySQL x64 for working with Kaspersky Security Center Linux

Do not make any manual changes to the Administration Server database and the IAM database, including modifying values, deleting or adding schemas, tables, indexes. Any changes to databases not performed by Administration Server itself disrupt the proper functioning of the Administration Server either immediately or later, for example, after upgrade to the newer version, or while restoring from a backup copy, and so on. Editing of databases is only permitted when you have received explicit instructions from Kaspersky Technical Support.
When uninstalling or migrating the Server to another device, you need to manually delete the database.

*To configure the DBMS account for the Administration Server installation:*

1. Run an environment for working with MySQL or MariaDB under the root account that you created when you installed the DBMS:

   ```
   sudo mysql -u root -p
   ```

2. Create internal DBMS user accounts with passwords. The installers of the Administration Server and Administration Server services use this internal DBMS user account for access to the database.

   Create an Administration Server user account named `kscdbadmin` and specify the password in `<password>`:

   ```
   CREATE USER 'kscdbadmin' IDENTIFIED BY '<password>';
   ```

3. Grant the following privileges to the created DBMS account:

   - Schema privileges:
     - Administration Server database: ALL (excluding GRANT OPTION)
     - System schemes (mysql and sys): SELECT, SHOW VIEW
     - The sys.table_exists stored procedure: EXECUTE
   - Global privileges for all schemes: PROCESS, SUPER.

   To grant the required privileges to the created DBMS account, run the following script:

   ```
   GRANT USAGE ON *.* TO 'kscdbadmin';
   GRANT ALL ON kav.* TO 'kscdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';
   ```

```
GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';
GRANT PROCESS ON *.* TO 'kscdbadmin';
GRANT SUPER ON *.* TO 'kscdbadmin';
```

If you use MariaDB 10.5 or earlier as a DBMS, you do not need to grant the EXECUTE privilege. In this case, exclude the following command from the script:

```
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin'.
```

4. To view the list of privileges granted to the DBMS account, run the following command:

   ```
   SHOW grants for 'kscdbadmin';
   ```

5. Create an IAM server account named `iamdbadmin` and specify the password in `<password>`:

   ```
   CREATE USER 'iamdbadmin' IDENTIFIED BY '<password>';
   ```

   If you use MySQL 8.0 or earlier as a DBMS, note that for these versions the "Caching SHA2 password" authentication is not supported. Change the default authentication from "Caching SHA2 password" to "MySQL native password":

   - To create a DBMS account that uses the "MySQL native password" authentication, execute the following command:

     ```
     CREATE USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
     ```

   - To change the authentication for an existing DBMS account, execute the following command:

     ```
     ALTER USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
     ```

6. Grant the following privileges to the created DBMS account:

   - Schema privileges:
     - Administration Server database: ALL (excluding GRANT OPTION)
     - System schemes (mysql and sys): SELECT, SHOW VIEW
     - The sys.table_exists stored procedure: EXECUTE
   - Global privileges for all schemes: PROCESS, SUPER.

   To grant the required privileges to the created DBMS account, run the following script:

   ```
   GRANT USAGE ON *.* TO 'iamdbadmin';
   GRANT ALL ON iam.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
   GRANT PROCESS ON *.* TO 'iamdbadmin';
   GRANT SUPER ON *.* TO 'iamdbadmin';
   ```

   If you use MariaDB 10.5 or earlier as a DBMS, you do not need to grant the EXECUTE privilege. In this case, exclude the following command from the script: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin'`.

7. To view the list of privileges granted to the DBMS account, execute the following command:
   `SHOW grants for 'iamdbadmin';`
8. Create an Administration Server database (in this example, the name is *kav*) by running the following command:
   `CREATE DATABASE kav`
   Use the same database name that you specified at the DBMS user account creation step.
9. Create an IAM database (in this example, the IAM database name is *iam*):
   `CREATE DATABASE iam`

**Example of the basic commands of the instructions**

```
administrator@ksclinux:~$ sudo mysql -u root -p

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 8

Server version: 8.4.11-0ubuntu0.26.04.1 (Ubuntu)

Copyright (c) 2000, 2026, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its

affiliates. Other names may be trademarks of their respective

owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE USER 'kscdbadmin' IDENTIFIED BY 'Your_P@$$w0rd';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT USAGE ON *.* TO 'kscdbadmin';

ON mysql.* TO 'kscdbadmin';

GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';

GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';

GRANT PROCESS ON *.* TO 'kscdbadmin';

GRANT SUPER ON *.* TO 'kscdbadmQuery OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL ON kav.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';
```

```
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';

in';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT PROCESS ON *.* TO 'kscdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SUPER ON *.* TO 'kscdbadmin';

Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> SHOW grants for 'kscdbadmin';

+-------------------------------------------------------------------+

| Grants for kscdbadmin@% |

+-------------------------------------------------------------------+

| GRANT PROCESS, SUPER ON *.* TO `kscdbadmin`@`%` |

| GRANT ALL PRIVILEGES ON `kav`.* TO `kscdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `mysql`.* TO `kscdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `sys`.* TO `kscdbadmin`@`%` |

| GRANT EXECUTE ON PROCEDURE `sys`.`table_exists` TO `kscdbadmin`@`%` |

+-------------------------------------------------------------------+

5 rows in set (0.00 sec)

mysql> CREATE USER 'iamdbadmin' IDENTIFIED BY 'Your_P@$$w0rd';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT USAGE ON *.* TO 'iamdbadmin';

'iamdbadmin';

GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';

GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
```

```
GRANT PROCESS ON *.* TO 'iamdbadmin';

GRANT SUPER ON *.* TO 'iamdbaQuery OK, 0 rows affected (0.01 sec)

mysql> GRANT ALL ON iam.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';

dmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.02 sec)

mysql> GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';

Query OK, 0 rows affected (0.01 sec)

mysql> GRANT PROCESS ON *.* TO 'iamdbadmin';

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SUPER ON *.* TO 'iamdbadmin';

Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> SHOW grants for 'iamdbadmin';

+-----------------------------------------------------------------------+

| Grants for iamdbadmin@% |

+-----------------------------------------------------------------------+

| GRANT PROCESS, SUPER ON *.* TO `iamdbadmin`@`%` |

| GRANT ALL PRIVILEGES ON `iam`.* TO `iamdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `mysql`.* TO `iamdbadmin`@`%` |

| GRANT SELECT, SHOW VIEW ON `sys`.* TO `iamdbadmin`@`%` |

| GRANT EXECUTE ON PROCEDURE `sys`.`table_exists` TO `iamdbadmin`@`%` |

+-----------------------------------------------------------------------+

5 rows in set (0.00 sec)

mysql> CREATE DATABASE kav;
```

```
Query OK, 1 row affected (0.01 sec)

mysql> CREATE DATABASE iam;

Query OK, 1 row affected (0.01 sec)

mysql> exit

Bye

administrator@ksclinux:~$
```

## Creating PostgreSQL-based databases and user accounts

Before granting rights to the DBMS account, make sure that the PostgreSQL DBMS server is configured to work with Kaspersky Security Center Linux.

The Ident authentication method is not supported.

Do not make any manual changes to the Administration Server database and the IAM database, including modifying values, deleting or adding schemas, tables, indexes. Any changes to databases not performed by Administration Server itself disrupt the proper functioning of the Administration Server either immediately or later, for example, after upgrade to the newer version, or while restoring from a backup copy, and so on. Editing of databases is only permitted when you have received explicit instructions from Kaspersky Technical Support.
When uninstalling or migrating the Server to another device, you need to manually delete the databases of the Administration Server and the IAM.

*To create databases and configure DBMS user accounts for installing Kaspersky Security Center Linux:*

1. Run the environment for managing the DBMS:

   `sudo -i -u postgres psql`

2. Log in under the *Postgres* user in the *Postgres* database.

3. Create the Postgres role for managing the Administration Server database (in this example, the `kscdbadmin` role):

   `CREATE USER "kscdbadmin" WITH PASSWORD '<password>';`

4. Create an Administration Server database (in this example, the Administration Server database name is `kav`):

   `CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

   We recommend specifying the Postgres role created at step 3 of these instructions as the owner of the Administration Server database (in this example, the role is `kscdbadmin`, and the password is `<password>`).

   **Specifying another user as the database owner**

   If you need to specify another Postgres role, connect to the Administration Server database with this owner role (or the superuser role) and run the following commands:

   ```
   GRANT ALL PRIVILEGES ON DATABASE "kav" TO "kscdbadmin";
   GRANT USAGE ON SCHEMA public TO "kscdbadmin";
   GRANT CREATE ON SCHEMA public TO "kscdbadmin";
   ```

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "kscdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "kscdbadmin";
```

Ensure that the Administration Server database owner role has the CONNECT and TEMPORARY privileges.

If the error "New encoding (UTF8) is incompatible with the encoding of the template database" occurs, create a database by using the command:
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin" TEMPLATE template0;`
instead of:
`CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

5. Create a Postgres role for managing the IAM database (in this example, the Postgres role is `iamdbadmin`):

```
CREATE USER "iamdbadmin" WITH PASSWORD '<password>';
```

6. Create an IAM database (in this example, the IAM database name is `iam`):

```
CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

The name of the IAM database must be different from the database that you installed to manage the Administration Server database.

We recommend specifying the Postgres role created at step 5 of these instructions as the owner of the IAM database (in this example, the role is `iamdbadmin`, and the password is `<password>`).

**Specifying another user as the IAM database owner**

If you need to specify another Postgres role, connect to the IAM database with this role (or the superuser role) and run the following commands:

```
GRANT ALL PRIVILEGES ON DATABASE "iam" TO "iamdbadmin";
GRANT USAGE ON SCHEMA public TO "iamdbadmin";
GRANT CREATE ON SCHEMA public TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "iamdbadmin";
```

Ensure that the IAM database owner role has the CONNECT and TEMPORARY privileges.

If the error "New encoding (UTF8) is incompatible with the encoding of the template database" occurs, create a database by using the command:
`CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin" TEMPLATE template0;`
instead of:
`CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";`

**Example of the basic commands of the instructions**

```
administrator@ksclinux:~$ sudo -i -u postgres psql
psql (18.4 (Ubuntu 18.4-0ubuntu.0.26.04.1))
Type "help" to help.
postgres=# CREATE USER kscdbadmin WITH PASSWORD 'password';
CREATE ROLE
postgres=# CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";
CREATE DATABASE
postgres=# CREATE USER iamdbadmin WITH PASSWORD 'password';
CREATE ROLE
postgres=# CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
```

```
CREATE DATABASE
postgres=# exit
administrator@ksclinux:~$
```

# Moving data from a shared tablespace to a file-per-table tablespace in a MySQL or MariaDB DBMS

For a MySQL and MariaDB DBMS, you can store data in the following ways:

- As a shared tablespace, when the data of all user databases is stored in a single file (usually, in the `ibdata1` file).
- As a file-per-table tablespace, when for each table a separate data space is created as a separate file.

Using a shared tablespace increases the risk of tablespace fragmentation. Since it is not possible to perform a `SHRINK` operation, a file in a shared tablespace may take up about 90% of the disk space. This negatively affects the disk subsystem performance. Thus, it is useful to opt for a file-per-table tablespace.

This article describes how to move data from a shared tablespace to a file-per-table tablespace. If the MySQL or MariaDB DBMSs are also used by other applications, you have to move the databases of these applications to the file-per-table tablespace.

> We recommend performing this procedure only if you are using MySQL or MariaDB DBMSs for Administration Server.
> Moving data from a shared tablespace to a file-per-table tablespace may increase the load on the disk subsystem.

## Prerequisites

Before you start, make sure that:

- You created a backup copy of Administration Server data by running either a data backup task or the klbackup utility.
- You created a backup copy of other applications whose databases are managed by MySQL or MariaDB DBMS (if any).
- On the device with the DBMS installed, in the partition with database, there is free disk space.

The required disk space is 150% of the current total databases size (current size of the `ibdata1` file).

Process

*To move data from a shared tablespace to a file-per-table tablespace:*

1. Stop the Kaspersky Security Center Administration Server service and other applications using the instance of the DBMS for which you want to perform this procedure.

2. Depending on the DBMS version, log in to your DBMS as a superuser, and then in any convenient application, run the `fix_tablespace.sql` script.

   You can view the `fix_tablespace.sql` scripts by clicking these links:

   **View the script for MySQL 5.7 and MariaDB 10.1+**

```
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;
```

   **View the script for MySQL 8.0+**

```
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;
```

You must not stop the script execution.
If no DBMS errors occurred, but you terminated the script execution, either run the script again or stop performing the steps of this procedure, restart the DBMS service, and restore the Administration Server data from the backup.

3. In the `[mysqld]` section of the my.cnf file, set the `innodb_file_per_table` parameter to `1`.
4. Restart the MySQL or MariaDB service.
5. Start the Kaspersky Security Center Administration Server service.

The data is moved from a shared tablespace to a file-per-table tablespace.

# Certificates for work with Kaspersky Security Center Linux

This section contains information about Kaspersky Security Center Linux certificates and describes how to issue and replace certificates for Kaspersky Security Center Web Console and how to renew a certificate for Administration Server if the Server interacts with Kaspersky Security Center Web Console.

## About Kaspersky Security Center certificates

Kaspersky Security Center uses the following types of certificates to enable a secure interaction between the application components:

- Administration Server certificate
- Mobile certificate
- Web Server certificate
- Kaspersky Security Center Web Console certificate
- Identity and Access Manager certificate

By default, Kaspersky Security Center uses self-signed certificates (that is, certificates issued by Kaspersky Security Center itself). If necessary, you can replace the self-signed certificates with user certificates in accordance to your organization's security standards. When using a custom certificate, the certificate file must include the full chain of public keys, including all intermediate certificates up to the root Certificate Authority (CA). After Administration Server verifies whether a custom certificate meets all applicable requirements, this certificate assumes the same functional scope as a self-signed certificate. The only difference is that the self-signed certificate is automatically reissued by the Administration Server, whereas with a user certificate, you need to reissue it manually after its expires. You can replace certificates with user certificates using the klsetsrvcert utility or in the Administration Server properties section in Kaspersky Security Center Web Console, depending on the certificate type. When you use the klsetsrvcert utility, you need to specify a certificate type by using one of the following values:

- C—Common certificate for ports 13000 and 13291.
- CR—Common reserve certificate for ports 13000 and 13291.
- M—Mobile certificate for port 13292.
- MR—Mobile reserve certificate for port 13292.
- MCA—Mobile certification authority for auto-generated user certificates.

The maximum validity period for any of the Administration Server certificates must be 397 days or less.

Administration Server certificates

An Administration Server certificate is required for the following purposes:

- Authentication of Administration Server when Kaspersky Security Center Web Console connects to it.
- Secure interaction between Administration Server and Network Agent on managed devices.
- Authentication when the primary Administration Servers are connected to secondary Administration Servers.

The Administration Server certificate is created automatically during installation of the Administration Server component and it is stored in the /var/opt/kaspersky/klnagent_srv/1093/cert/ directory. You specify the Administration Server certificate when you create a response file to install Kaspersky Security Center Web Console. This certificate is called common ("C"). After installing Kaspersky Security Center Web Console, the certificate you specified is copied to the /var/opt/kaspersky/ksc-web-console/certificates/external directory.

The Administration Server certificate is valid for 397 days. Kaspersky Security Center automatically creates a common reserve ("CR") certificate 90 days before the expiration of the common certificate. The common reserve certificate is subsequently used for seamless replacement of the Administration Server certificate. When the common certificate is about to expire, the common reserve certificate is used to maintain the connection with Network Agent instances installed on managed devices. With this purpose, the common reserve certificate automatically becomes the new common certificate 24 hours before the old common certificate expires.

The maximum validity period for any of the Administration Server certificates must be 397 days or less.

If necessary, you can assign a custom certificate for the Administration Server. For example, this may be necessary for better integration with the existing PKI of your enterprise or for custom configuration of the certificate fields. When the certificate is replaced, all Network Agents that were previously connected to Administration Server through SSL lose their connection and return "Administration Server authentication error." To eliminate this error, you will have to restore the connection after the certificate replacement.

If the Administration Server certificate is lost, you must reinstall the Administration Server component, and then restore the data in order to recover it.

You can also back up the Administration Server certificate separately from other Administration Server settings in order to move Administration Server from one device to another without reconnecting Network Agents.

If you open Kaspersky Security Center Web Console in different browsers and download the Administration Server certificate file in the Administration Server properties window, the downloaded files have different names.

### Mobile certificates

A mobile certificate ("M") is required for authentication of the Administration Server on mobile devices. You specify the mobile certificate in the Administration Server properties.

Also, a mobile reserve ("MR") certificate exists: it is used for seamless replacement of the mobile certificate. Kaspersky Security Center automatically generates this certificate 90 days before the expiration of the mobile certificate. When the mobile certificate is about to expire, the mobile reserve certificate is used to maintain the connection with Network Agent instances installed on managed mobile devices. With this purpose, the mobile reserve certificate automatically becomes the new mobile certificate 24 hours before the old mobile certificate expires.

If the connection scenario requires the use of a client certificate on mobile devices (connection involving two-way SSL authentication), you can generate those certificates by means of the certificate authority for auto-generated user certificates ("MCA"). Also, in the Administration Server properties, you can specify custom client certificates issued by a certification authority, while integration with the domain Public Key Infrastructure (PKI) of your organization enables you to issue client certificates by means of your domain certification authority.

Also, for authentication of Administration Server on mobile devices running the iOS operating system an iOS MDM Server certificate is required. For more information, see Configuring an iOS MDM Server certificate.

### Web Server certificate

Web Server, a component of Kaspersky Security Center Administration Server, uses a special type of certificate. This certificate is required for publishing Network Agent installation packages that you subsequently download to managed devices, as well as for Kaspersky Security for Mobile installation packages. For this purpose, Web Server can use various certificates.

If the mobile device support is disabled, Web Server uses one of the following certificates, in order of priority:

1. Custom Web Server certificate that you specified manually by means of Administration Console
2. Common Administration Server certificate ("C")

If the mobile device support is enabled, Web Server uses one of the following certificates, in order of priority:

1. Custom Web Server certificate that you specified manually by means of Administration Console
2. Custom mobile certificate
3. Self-signed mobile certificate ("M")
4. Common Administration Server certificate ("C")

### Kaspersky Security Center Web Console certificate

The Server of Kaspersky Security Center Web Console (hereinafter referred to as Web Console) has its own certificate. When you visit a website, the browser verifies whether the connection is trusted. The Web Console certificate allows you to authenticate the Web Console and is used to encrypt traffic between a browser and the Web Console.

When you open the Web Console, the browser may inform you that the connection to the Web Console is not private and the Web Console certificate is invalid. This warning is displayed because the Kaspersky Security Center Web Console certificate is self-signed and automatically generated by Kaspersky Security Center. To remove this warning, you can do one of the following:

- Replace the Web Console certificate with a custom one (recommended option). Create a certificate that is trusted in your infrastructure and that meets the requirements for custom certificates.
- Add the Web Console certificate to the list of trusted browser certificates. We recommend that you use this option only if you cannot create a custom certificate.

By default, a self-signed certificate is valid for 30 days. You can change this value in the file in the web console configuration file, /var/opt/kaspersky/ksc-web-console/server/config.json. To apply the specified value, you need to restart the Web Console process.

The Web Console automatically reissues this certificate and switches to it before the expiration date of the self-signed certificate.

You can replace the self-signed Web Console certificate with a user certificate.

### Identity and Access Manager certificate

An Identity and Access Manager certificate (IAM certificate) is required for the following purposes:

- Authentication of Administration Server when a user's browser connects to it over the OAuth protocol.
- Authentication of Administration Server when Kaspersky Security Center Web Console connects to it.

The IAM certificate is created automatically the first time you run Administration Server. The certificate is stored on the Administration Server device in the directory: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem (for Kaspersky Security Center failover cluster: <shared data folder>/iam/main_certificate.pem). You must specify the path to the IAM certificate by using the `iamCertPath` parameter when you create a response file for installing Kaspersky Security Center Web Console.

The IAM certificate is valid for 365 days. Kaspersky Security Center automatically creates a reserve IAM certificate 48 hours before the expiration of the current certificate. The reserve certificate is subsequently used for seamless replacement of the expired IAM certificate.

The maximum validity period for any IAM certificate must be 397 days or less.

If necessary, you can assign a custom IAM certificate. For example, this may be necessary for better integration with the existing PKI of your enterprise or for custom configuration of the certificate fields.

When you signing in to Kaspersky Security Center Web Console, the browser is redirected to the Administration Server login page (https://<Administration Server address>:4444) for authentication. The traffic between the browser and Administration Server is encrypted by using the TLS protocol and the IAM certificate.

The browser may inform you that the connection to Administration Server is not private and the IAM certificate is invalid. This warning appears because the IAM certificate is self-signed and automatically generated by Kaspersky Security Center. To remove this warning, you can do one of the following:

- Replace the IAM certificate with a custom one (recommended option). Create a certificate that is trusted in your infrastructure and that meets the requirements for custom certificates.
- Add the IAM certificate to the list of trusted browser certificates. We recommend that you use this option only if you cannot create a custom certificate.

## Requirements for custom certificates used in Kaspersky Security Center Linux

The table below shows the requirements for custom certificates specified for different components of Kaspersky Security Center Linux.

Requirements for Kaspersky Security Center Linux certificates

| Certificate type | Requirements | Comments |
|---|---|---|
| Common certificate, Common reserve certificate ("C", "CR") | Minimum key length: 2048.<br>Basic constraints:<br>• Path Length Constraint: None<br>Key Usage:<br>• Digital signature<br>• Certificate signing<br>• Key encryption<br>• CRL Signing<br>Extended Key Usage (optional): server authentication, client authentication.<br>The certificate must include a valid Subject Alternative Name (SAN) that contains the Administration Server loopback address:<br>• For IPv4: 127.0.0.1<br>• For IPv6: 0:0:0:0:0:0:0:1 | Extended Key Usage parameter is optional.<br>Path Length Constraint value may be an integer different from "None," but not less than 1. |
| Web Server certificate | Extended Key Usage: server authentication.<br>The PKCS #12 / PEM container from which the certificate is specified includes the full chain of public keys.<br>The Subject Alternative Name (SAN) of the certificate is present; that is, the value of the `subjectAltName` field is valid.<br>The certificate meets the effective requirements of browsers imposed on server certificates, as well as the current baseline requirements of the CA/Browser Forum. | — |

| Certificate type | Requirements | Comments |
| --- | --- | --- |
| Kaspersky Security Center Web Console certificate | Extended Key Usage (EKU): server authentication.<br>The PEM container from which the certificate is specified includes the full chain of public keys.<br>The Subject Alternative Name (SAN) of the certificate is present; that is, the value of the `subjectAltName` field is valid. The value must match the IAM address specified when installing the Administration Server. To obtain the specified IAM address, run the following command on the device with Administration Server installed:<br>`grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`<br>The certificate meets the effective requirements of browsers to server certificates, as well as the current baseline requirements of the CA/Browser Forum. | Encrypted certificates are not supported by Kaspersky Security Center Web Console. |
| Identity and Access Manager certificate (IAM certificate) | Extended Key Usage: server authentication.<br>The PEM container from which the certificate is specified includes the full chain of public keys.<br>The certificate meets the effective requirements of browsers to server certificates, as well as the current baseline requirements of the CA/Browser Forum. | Encrypted certificates are not supported by Kaspersky Security Center Web Console. |

# Reissuing the internal certificates for Kaspersky Security Center Web Console

Kaspersky Security Center Web Console uses the following certificates:

- A public certificate (Web Console TLS certificate), which the Web Console presents to the browser for an HTTPS connection.
- An internal certificate that the Web Console uses for TLS connections.

## Public certificate

Most browsers impose a limit on the validity term of a certificate. To match this limit, the validity term of the Kaspersky Security Center Web Console public certificate is limited to 30 days. You can replace an existing certificate received from a certification authority (CA) by issuing a new self-signed certificate manually.

When you open the Kaspersky Security Center Web Console, the browser may inform you that the connection to the Kaspersky Security Center Web Console is not private and the Kaspersky Security Center Web Console certificate is invalid. This warning appears because the Kaspersky Security Center Web Console certificate is self-signed and automatically generated by Kaspersky Security Center. To remove or prevent this warning, you can do one of the following:

- Replace the Web Console self-signed public certificate with a user certificate (recommended option). Create a certificate that is trusted in your infrastructure and that meets the requirements for custom certificates.
- Add the Kaspersky Security Center Web Console certificate to the list of trusted browser certificates. We recommend that you use this option only if you cannot create a custom certificate.

## Internal certificate

The internal Web Console certificate is used only for internal mutual authentication of Web Console components and is not displayed to the user.

By default, the validity period of the internal certificate of Kaspersky Security Center Web Console is 3 years (1095 days).

14 days before the specified term expires, the Web Console displays a notification reminding you to reissue the internal certificate.

*To reissue the expired internal certificate of Kaspersky Security Center Web Console:*

Reinstall Kaspersky Security Center Web Console by performing one of the following:

- If you want to use the same installation file of Kaspersky Security Center Web Console, remove Kaspersky Security Center Web Console, and then install the same Kaspersky Security Center Web Console version.
- If you want to use an installation file of an upgraded version, run the upgrade command.

The Kaspersky Security Center Web Console certificate is reissued.

## Replacing certificate for Kaspersky Security Center Web Console

By default, when you install Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console), a browser certificate for the application is issued automatically. You can replace the automatically generated certificate with a custom one.

*To assign a Kaspersky Security Center Web Console user certificate:*

1. Save the file with the certificate and the file with the private key in the following directory:

   /var/opt/kaspersky/ksc-web-console/certificates/external/

   Supported file format: PEM.
   Reading and writing to the directory requires root privileges. The user that the interactive web console service runs as only has the read permission.

2. Name the files as follows:

   - web-console.crt: the file with the certificate.
   - web-console.key: the file with the private key without a password.

A custom primary certificate is assigned and Web Console is using it.

If you want to replace the user certificate:

- If you want to replace the user certificate with another user certificate, follow the same instructions.
- If you want to replace the user certificate with a self-signed certificate, delete one or both of the user certificate files.

When a user certificate expires, the Web Console displays a corresponding notification and continues to use the expired certificate.

If the user primary certificate that you specified is invalid, the Web Console displays a corresponding notification, releases a self-signed primary certificate, and switches to it.

The notification is first displayed 14 days before the certificate expires.

## Converting a PFX certificate to the PEM format

To use a PFX certificate in Kaspersky Security Center Web Console, you must first convert it to the PEM format by using any convenient OpenSSL-based cross-platform utility.

*To convert a PFX certificate to the PEM format in the Linux operating system:*

1. In an OpenSSL-based cross-platform utility, execute the following commands:

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Make sure that the certificate file and the private key are generated to the same directory where the .pfx file is stored.

3. Kaspersky Security Center Web Console does not support passphrase-protected certificates. Therefore, run the following command in an OpenSSL-based cross-platform utility to remove a passphrase from the .pem file:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Do not use the same name for the input and output .pem files.

   As a result, the new .pem file is unencrypted. You do not have to enter a passphrase to use it.

The .crt and .pem files are ready to use, so you can specify them in the Kaspersky Security Center Web Console installer.

## Scenario: Specifying the custom Administration Server certificate

You can assign the custom Administration Server certificate, for example, for better integration with the existing public key infrastructure (PKI) of your enterprise or for custom configuration of the certificate fields. It is useful to replace the certificate immediately after installation of Administration Server and before the quick start wizard finishes.

> The maximum validity period for any of the Administration Server certificates must be 397 days or less.

Prerequisites

The following conditions must be met:

- The new certificate must be created in the PKCS#12 format (for example, by means of the organization's PKI).
- For the new certificate, the requirements listed in the table below must be met.

  In the following table, take note of the "CA: true" requirement. It means that the new certificate must be issued by a trusted certificate authority (CA). The new certificate with the requirement "CA: true" must include the entire chain of trust and a private key, which must be stored in a file with the pfx or p12 extension.

Requirements for the Administration Server certificates

| Certificate type | Requirements |
|---|---|
| Common certificate, common reserve certificate ("C", "CR") | Minimum key length: 2048.<br>Basic constraints:<br>• Path Length Constraint: None<br>Path Length Constraint value may be an integer different from "None," but not less than 1.<br>Key Usage:<br>• Digital signature<br>• Certificate signing<br>• Key encryption<br>• CRL Signing<br>Extended Key Usage (EKU): server authentication and client authentication. The EKU is optional, but if your certificate contains it, the server and client authentication data must be specified in the EKU.<br><br>The certificate must include a valid Subject Alternative Name (SAN) that contains the Administration Server loopback address:<br>• For IPv4: 127.0.0.1<br>• For IPv6: 0:0:0:0:0:0:0:1 |
| Mobile certificate, mobile reserve certificate ("M", "MR") | Minimum key length: 2048.<br>Basic constraints:<br>• CA: true<br>• Path Length Constraint: None<br>Path Length Constraint value may be an integer different from "None", if Common certificate has a Path Length Constraint value not less than 1.<br>Key Usage:<br>• Digital signature<br>• Certificate signing<br>• Key encryption<br>• CRL Signing<br>Extended Key Usage: server authentication. The EKU is optional, but if your certificate contains it, the server authentication data must be specified in the EKU. |

| Certificate type | Requirements |
| --- | --- |
| Certificate CA for auto-generated user certificates ("MCA") | Minimum key length: 2048.<br>Basic constraints:<br>• CA: true<br>• Path Length Constraint: None<br>Path Length Constraint value may be an integer different from "None", if Common certificate has a Path Length Constraint value not less than 1.<br>Key Usage:<br>• Digital signature<br>• Certificate signing<br>• Key encryption<br>• CRL Signing<br>Extended Key Usage (EKU): client authentication. The EKU is optional, but if your certificate contains it, the client authentication data must be specified in the EKU. |

Certificates issued by a public CA do not have the certificate signing permission. To use such certificates, make sure that you installed Network Agent version 13 or later on distribution points or connection gateways in your network. Otherwise, you will not be able to use certificates without the signing permission.

## Stages

Specifying the Administration Server certificate proceeds in stages:

1. **Replacing the Administration Server certificate**

   Use the command-line klsetsrvcert utility for this purpose.

2. **Specifying a new certificate and restoring connection of Network Agents to the Administration Server**

   When the certificate is replaced, all Network Agents that were previously connected to Administration Server through SSL lose their connection and return "Administration Server authentication error." To specify the new certificate and restore the connection, use the command-line klmover utility.

3. **Specifying a new certificate in the certificates directory of Kaspersky Security Center Web Console**

   Save the file with the Administration Server certificate in the directory: /var/opt/kaspersky/ksc-web-console/certificates/external/

   Name the file <address>-admin-server.crt, where <address> is the address of the Administration Server that you specified in the `iamHost` setting of the Web Console installer answers file.

   Supported file format: PEM.
   Reading and writing to the directory requires root privileges. The user that the interactive web console service runs as only has the read permission.

## Results

When you finish the scenario, the Administration Server certificate is replaced and the server is authenticated by Network Agents on the managed devices.

# Replacing the Administration Server certificate by using the klsetsrvcert utility

To avoid losing control of devices, refer to the Scenario: Specifying the custom Administration Server certificate before proceeding.

*To replace the Administration Server certificate:*

From the command line, run the following utility:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert [-t <certificate type> {-i <path to new certificate> [-p <password>] [-o
<validation parameters>] | -g <dns name>}][-f <replacement time>][-r <root certificates>][-l <log file path>]
```

The description of the klsetsrvcert utility parameters is presented in the table below.

Values of the klsetsrvcert utility parameters

| Setting | Value |
|---|---|
| `-t < certificate type >` | Type of certificate to be replaced. Possible values of the `< certificate type >` parameter:<br>• `C` —Replace the common certificate for ports 13000 and 13291.<br>• `CR` —Replace the common reserve certificate for ports 13000 and 13291. |
| `-f < replacement time >` | Schedule for changing the certificate, using the format "DD-MM-YYYY hh:mm" (for ports 13000 and 13291).<br>Use this parameter if you want to replace the common certificate with the common reserve certificate before the common certificate expires.<br>Specify the time when managed devices must synchronize with Administration Server on a new certificate. |
| `-i < path to new certificate >` | Container with the certificate and a private key in the PKCS#12 format (file with the .p12 or .pfx extension). |
| `-p < password >` | Password used for protection of the p12 container.<br>The certificate and a private key are stored in the container, therefore, the password is required to decrypt the file with the container. |
| `-o < validation parameters >` | Certificate validation parameters (semicolon separated).<br>To use a custom certificate without signing permission, specify `-o NoCA` in the klsetsrvcert utility. This is useful for certificates issued by a public CA.<br>To change encryption key length for certificate types C or CR, specify `-o RsaKeyLen:< key length >` in the klsetsrvcert utility, where `< key length >` parameter is the required key length value. Otherwise, the current certificate key length is used. |
| `-g < dns name >` | A new certificate will be created for the specified DNS name (Common Name and Subject Alternative Name). |
| `-r < root certificates >` | Trusted root Certificate Authority list, format PEM. |
| `-l < log file path >` | Results output file. By default, the output is redirected into the standard output stream. |

For example, to specify the custom Administration Server certificate, use the following command:

```
klsetsrvcert -t C -i <path to new certificate> -p <password> -o NoCA
```

After the certificate is replaced, all Network Agents connected to Administration Server through SSL lose their connection. To restore it, use the command-line klmover utility.

To avoid losing the Network Agents connections, use the following commands:

1. To install the new certificate,

```
klsetsrvcert -t CR -i <path to new certificate> -p <password> -o NoCA
```

2. To specify the date when the new certificate will be applied,

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

where "`DD-MM-YYYY hh:mm`" is the date 3–4 weeks later than the current date. The time shift for changing the certificate to the new one will allow the new certificate to be distributed to all Network Agents.

Questions & Answers

**What additional steps are required after replacing the Administration Server common certificate?**

1. Ensure that the **requirements for custom certificates are met**.

   If you are using custom certificate instead of the self-signed one, before upgrading Kaspersky Security Center Linux to the later version, you have to make sure that the certificate includes the Subject Alternative Name (SAN). If not, is important to replace the certificate before upgrading Kaspersky Security Center Linux. Otherwise, you will not be able to sign in to Web Console after upgrade.

   *To make sure that the certificate includes SAN:*

   1. On the device with Administration Server installed, execute the command:

      - For a Linux-based device:

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - For a Windows-based device:

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. Make sure that the Subject Alternative Name (SAN) is present in the command output and contains the address of the Administration Server device.

   3. If the Subject Alternative Name is missing, use the klsetsrvcert utility to replace your user certificate with a certificate that meets the requirements.

2. Ensure that the IAM Server configuration file contains the current Administration Server address. If not, add the address to the configuration file.

3. Reinstall the Web Console to avoid the following error:

   *Administration Server uses an untrusted certificate. Please reconfigure the application by specifying a valid certificate, or contact the main administrator.*

# Connecting Network Agents to Administration Server by using the klmover utility

You can use the klmover utility to restore connection from uncontrolled devices to Administration Server, for example, after an Administration Server failure, if it is not possible to restore it from a backup.

*To restore the connection, run the klmover utility from the command line:*

- For Linux:
  - For 32-bit systems: `/opt/kaspersky/klnagent/bin/klmover [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-nossl] [-cert <path to certificate file>]`
  - For 64-bit systems: `/opt/kaspersky/klnagent64/bin/klmover [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-nossl] [-cert <path to certificate file>]`
- For Windows:
  - For 32-bit systems: `<path>\klmover.exe [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-nossl] [-cert <path to certificate file>]`
  - For 64-bit systems: `<path>\klmover.exe [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-nossl] [-cert <path to certificate file>]`
- For macOS:

  `/Library/Application Support/Kaspersky Lab/klnagent/Binaries/klmover [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-nossl] [-cert <path to certificate file>]`

  where `<path>` is the default installation path for Network Agent or the installation path specified by you in the settings of the Network Agent installation package.

To prevent intruders from moving devices out of your Administration Server's control, we strongly recommend enabling password protection for running the klmover utility. To enable password protection, select the **Use uninstallation password** option in the Network Agent policy settings.

If you lose or forget the password from the password-protected Network Agent installed on the device that is no longer under the management of Kaspersky Security Center Linux, you cannot remove Network Agent by using the klmover utility or the command line. In this case, you have to reinstall the operating system on the device with the installed password-protected Network Agent.

The klmover utility requires local administrator rights.

Enabling the **Use uninstallation password** option on Windows devices also enables password protection for the Cleaner tool (cleaner.exe).

You cannot use the klmover utility for client devices connected to Administration Server through connection gateways. For such devices you have to either reconfigure Network Agent or reinstall Network Agent and specify connection gateway.

The description of the klmover utility parameters is presented in the table below.

Values of the klmover utility parameters

| Setting | Value |
|---|---|
| `-address < server address >` | Address of the Administration Server for connection.<br>You can specify an IP address or the DNS name. |
| `-pn < port number >` | Number of the port through which non-encrypted connection to the Administration Server is established.<br>The default port number is 14000. |
| `-ps < SSL port number >` | Number of the SSL port through which encrypted connection to the Administration Server is established by using SSL.<br>The default port number is 13000. |
| `-nossl` | Use non-encrypted connection to the Administration Server.<br>If the key is not in use, Network Agent is connected to the Administration Server by using encrypted SSL protocol. |
| `-cert < path to certificate file >` | Use the specified certificate file for authentication of access to Administration Server. |
| `-nauninstpwd < password >` | Use this parameter to specify the Network Agent uninstallation password.<br>Optional setting. |

# Reissuing the Web Server certificate

The Web Server certificate used in Kaspersky Security Center Linux is required for publishing Network Agent installation packages that you subsequently deliver to managed devices, as well as for publishing iOS MDM profiles, iOS apps, and Kaspersky Endpoint Security for Mobile installation packages. Depending on the current application configuration, various certificates can function as the Web Server certificate (for more detail, see About Kaspersky Security Center Linux certificates).

You may need to reissue the Web Server certificate to meet the specific security requirements of your organization or to maintain continuous connection of your managed devices before starting to upgrade the application. Kaspersky Security Center provides two ways of reissuing the Web Server certificate. The choice between the two methods depends on whether you have mobile devices connected and managed through the mobile protocol (i.e., by using the mobile certificate).

If you have never specified your own custom certificate as the Web Server certificate in the **Web Server** section of the Administration Server properties window, the mobile certificate acts as the Web Server certificate. In this case, the Web Server certificate reissuance is performed through the reissuance of the mobile protocol itself.

*To reissue the Web Server certificate when you have any mobile devices managed through the mobile protocol:*

1. Generate your custom certificate and prepare it for the usage in Kaspersky Security Center Linux. Check whether your custom certificate meets the requirements of Kaspersky Security Center Linux. If necessary, modify the certificate.

2. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

3. On the **General** tab, select the **Web Server** section.

4. In the **Over HTTP** subsection, select the **Upload certificate from file** option and click the **Change certificate** button.

5. In the window that opens, in the **Certificate format** field select the type of your certificate:

   - If you have selected **PKCS #12 container**, click the **Browse** button next to the **Certificate** field and specify the certificate file on your hard drive. If the certificate file is password-protected, enter the password in the **Password** field.

   - If you have selected **X.509 certificate**, click the **Browse** button next to the **Private key** field and specify the private key on your hard drive. If the private key is password-protected, enter the password in the **Password** field.

6. Click the **Save** button, then click **OK**.

   The window is closed.

7. If necessary, in the **Web Server HTTPS port** field change the number of the HTTPS port for Web Server and click the **Save** button.

The Web Server certificate is reissued.

*To reissue the Web Server certificate when you have no mobile devices managed through the mobile protocol:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. In the **General** tab, select the **Certificates** section.

3. If you plan to continue using the certificate issued by Kaspersky Security Center, do the following:

   a. Select the **Certificate issued through Administration Server** option and click the **Browse** button.

   b. In the window that opens, in the **Connection address** and **Activation term** groups of settings, select the relevant options and click **OK**.

Alternatively, if you plan to use your own custom certificate, do the following:

a. Check whether your custom certificate meets the requirements of Kaspersky Security Center Linux. If necessary, modify the certificate.

b. Select the **Other certificate** option, click the **Manage certificate** button, and then in the window that opens, click the **Browse** button.

c. In the window that opens, in the **Certificate format** field select the type of your certificate:

- If you have selected **PKCS #12 container**, click the **Browse** button next to the **Certificate** field and specify the certificate file on your hard drive. If the certificate file is password-protected, enter the password in the **Password** field.
- If you have selected **X.509 certificate**, click the **Browse** button next to the **Private key** field and specify the private key on your hard drive. If the private key is password-protected, enter the password in the **Password** field.

d. Click the **Save** button, then click **OK**.

The mobile certificate is reissued to be used as the Web Server certificate.

## Changing the default IAM certificate to a custom one

*To assign a IAM user certificate:*

1. Generate your custom certificate and prepare it for the usage in Kaspersky Security Center Linux. Check whether your custom certificate meets the requirements of Kaspersky Security Center Linux.
2. Ensure that the kladmins group has access to IAM certificate files.
3. Locate the IAM configuration file: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   In this file, add paths to IAM certificate files to the `server_iam` section:

   - `certificates.main.cert`: Path to the primary certificate file.
   - `certificates.main.key`: Path to the private key of the primary certificate. The private key must not be password-protected.
4. Restart the kliam service by running the following command:

   ```
   sudo service kliam_srv restart
   ```
5. Save the IAM certificate file in the following directory:

   /var/opt/kaspersky/ksc-web-console/certificates/external/

   > Supported file format: PEM.
   > The user that the Kaspersky Security Center Web Console service is running as must have sufficient privileges to read files saved in the directory.
6. Give the file a name: <address>-iam-server.crt

   where <address> is the address of the IAM that you specified in the `iamHost` setting of the Web Console installer answers file.

An IAM user certificate is assigned and Web Console is using it.

If you need to replace the IAM user certificate, follow the same instructions.

If your IAM certificate is not valid and a new valid certificate has not been received, an error is displayed in the Web Console.

By default, a warning notification is displayed 14 days before the expiration of the current certificate. A critical notification is displayed 2 days before the expiration of the current certificate.

If IAM has switched to a reserve certificate after you had manually specified an IAM certificate (self-signed or user) for the Web Console, the Web Console automatically obtains the reserve IAM certificate and continues to connect to the Administration Server. The user certificate that you had specified remains in the /var/opt/kaspersky/ksc-web-console/certificates/external directory, but is not used.

*To change the reserve IAM certificate:*

1. Locate the IAM configuration file: `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   In this file, specify paths to IAM certificate files:

   - `server_iam.certificates.reserve.cert`: Path to the primary certificate file.
   - `server_iam.certificates.reserve.key`: Path to the private key of the primary certificate. The private key must not be password-protected.

2. Restart the kliam service by running the following command:

   ```
   sudo systemctl restart kliam_srv.service
   ```

   When the current certificate file expires, the reserve IAM certificate is used instead.

## Adding the Administration Server address to the IAM Server configuration

After changing the Common Administration Server certificate ("C") during an upgrade, relocation, or migration, you need to specify the Administration Server address in the IAM Server configuration file to ensure proper certificate validation between the IAM Server and Administration Server.

*To add the Administration server address to the IAM Server configuration:*

1. Get the Subject Alternative Name (SAN) value from the Common Administration Server certificate ("C") by running the following command:

   ```
   sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
   ```

2. Depending on the command output, do one of the following:

   - If the output indicates that the value is missing or contains only the network IP address, check the **user certificate requirements**.

     If you are using custom certificate instead of the self-signed one, before upgrading Kaspersky Security Center Linux to the later version, you have to make sure that the certificate includes the Subject Alternative Name (SAN). If not, is important to replace the certificate before upgrading Kaspersky Security Center Linux. Otherwise, you will not be able to sign in to Web Console after upgrade.

     *To make sure that the certificate includes SAN:*

     1. On the device with Administration Server installed, execute the command:

        - For a Linux-based device:

          ```
          sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -
          noout -ext subjectAltName
          ```

- For a Windows-based device:

  ```
  certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
  ```

2. Make sure that the Subject Alternative Name (SAN) is present in the command output and contains the address of the Administration Server device.

3. If the Subject Alternative Name is missing, use the klsetsrvcert utility to replace your user certificate with a certificate that meets the requirements.

If it does not meet the requirements, replace the Administration Server common certificate on the previous Administration Server by using the klsetsrvcert utility. After that, repeat the upgrade, relocation, or migration procedure.

- If the value matches the value specified during Kaspersky Security Center Linux installation (on the **Enter IAM Server DNS name** step of the installation wizard or, for silent installation, in the `KLSRV_UNATT_IAM_ADDRESS` parameter), no further action is required. The IAM Server and Administration Server will interact correctly.

- If the value contains DNS names or loopback addresses (127.0.0.1 and/or 0:0:0:0:0:0:0:1), use one of them in the configuration file. It is recommended to use 127.0.0.1.

3. Under `server_iam` in the IAM server configuration file, make sure that the `ksc_address: "<SAN_address>"` value is set to one of the SAN addresses in the general certificate of the Administration Server.

   You can use a text editor to modify the IAM Server configuration file, for example, vi. The following command opens the file in the vi text editor:

   ```
   vi /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

   Example of the server_iam block in the IAM Server configuration file:

   ```
   server_iam:
       iam_address: "ksc.example.com"
       server_display_name: "ksc.example.com"
       ksc_address: "oldksc.example.internal"
       ksc_ca: "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
   ```

   Make sure to use the same spacing as in the example.

4. Make sure the network name in the `ksc_address` setting resolved to the loopback address (127.0.0.1 or 0:0:0:0:0:0:0:1) of the Administration Server. To do this, you can use the Ping utility on the Administration Server.

   If the allowed address is different or the address cannot be resolved, add an line to the hosts file on the Administration Server.

5. Restart the IAM Server service to apply the configuration changes by running the following command:

   ```
   sudo systemctl restart kliam_srv.service
   ```

The Administration Server address is added to the IAM Server configuration file from the Administration Server common certificate.

Troubleshooting

Multiple Administration Servers with the same network name on the network and IAM server configuration issues may lead to errors when logging in to the Web Console. The table below describes possible errors and resolutions.

| Error | Description | Solution |
|---|---|---|
| Your request cannot be processed right now. Please wait and then try again. | In addition to the data initialization process after upgrading or restoring Kaspersky Security Center Linux, this error may occur if the connection to Administration Server by using the specified network address fails. | Check that the specified address resolves to the IP address of the current Administration Server. |
| Administration Server uses an untrusted certificate. Please reconfigure the application by specifying a valid certificate, or contact the main administrator. | The error may occur if the address value in the IAM Server configuration file does not match the value in the Subject Alternative Name (SAN) attribute of the Administration Server common certificate. | Follow the instructions above. |
| The user name or password is incorrect. | In addition to incorrect credentials, this error may occur if another Administration Server with the same name exists on the network. | Check that the specified address resolves to the IP address of the current Administration Server. |

# Defining a shared folder

After Administration Server installation, you can specify the location of the shared folder, in the Administration Server properties. By default, the shared folder is created on the device with Administration Server. However, in some cases (such as high load or a need for access from an isolated network), it is useful to locate the shared folder on a dedicated file resource.

The shared folder is used occasionally in Network Agent deployment.

Case sensitivity for the shared folder must be disabled.

# Signing in to Kaspersky Security Center Web Console and signing out

You can sign in to Kaspersky Security Center Web Console after you install the Administration Server and Web Console Server. You must know the web address of the Administration Server and the port number specified during installation (by default, the port is 8080). In your browser, JavaScript must be enabled.

You can sign in to Kaspersky Security Center Web Console by using the following methods:

- By using domain authentication (single sign-on)

  This method is used for secure authentication in Kaspersky Security Center Web Console connected to Administration Server version 16 and later. If you want to use domain authentication, you must specify additional parameters for interaction with Identity and Access Manager (IAM) during the Kaspersky Security Center Web Console installation.

- By specifying the name and password of the domain user

  Before you sign in by using a domain user account, poll the domain controller to obtain the list of domain users. Then, you have to specify the domain user name and password to sign in to the Administration Server. This method is supported for authentication only via Microsoft Active Directory.

- By specifying the name and password of the internal user

The user account you want to sign in with to the Kaspersky Security Center Web Console must have a role assigned. Before signing in, make sure that the domain or internal user account has been assigned a role. Otherwise, a login error will occur.

Signing in by using domain authentication (single sign-on)

*To sign in to Kaspersky Security Center Web Console by using domain authentication:*

1. In your browser, go to https://<Kaspersky Security Center Web Console address>:<Port number>.

   The Administration Server selection page is displayed.

2. If you added several trusted servers, in the Administration Servers list select the Administration Server that you want to connect to.

   If you only added a single Administration Server, the Administration Servers list is not displayed.

   The browser is redirected to https://<Administration Server address>:4444.

3. Configure Kerberos domain authentication.

4. Do one of the following:

   - Click the **Use domain authentication** button.

   - If one or more virtual Administration Servers are created on the Server and you want to sign in to a virtual Server by using domain authentication:

     a. Click **Show virtual Server options**.

     b. Type the virtual Administration Server name that you specified while creating the virtual Server.

     c. Click the **Use domain authentication** button.

5. Specify the one-time security code generated by the authenticator app on the mobile device.

   At the first sign-in, configure two-step authentication for your account. If two-factor authentication configuration is not available to you, contact a user who has the Modify object ACLs right in the **General features**: **User permissions** functional area and configured two-factor authentication to add your account to the two-factor authentication allowlist.

After sign-in, the Kaspersky Security Center Web Console home page is displayed, containing the language and theme that you used last time. You can navigate through Kaspersky Security Center Web Console and use it to work with Kaspersky Security Center Linux.

Signing in by specifying the name and password of the domain or internal user

*To sign in to Kaspersky Security Center Web Console by specifying the user name and password:*

1. In your browser, go to https://<Kaspersky Security Center Web Console address>:<Port number>.

   The Administration Server selection page is displayed.

2. If you added several trusted servers, in the Administration Servers list select the Administration Server that you want to connect to.

   If you only added a single Administration Server, the Administration Servers list is not displayed.

   The browser is redirected to https://<Administration Server address>:4444.

3. Do one of the following:

   - To sign in to the Administration Server with a domain user account, enter the user name and password of the domain user.

     You can enter the user name of the domain user in one of the following formats:

     - Username@dns.domain
     - NTDOMAIN\Username

     Before you sign in with a domain user account, poll the domain controller to obtain the list of domain users.

   - To sign in to the Administration Server by specifying the administrator's user name and password, enter the user name and password of the internal user.
   - If one or more virtual Servers are created on the Server and you want to sign in to a virtual Server:

     a. Click **Show virtual Server options**.

     b. Type the virtual Administration Server name that you specified while creating the virtual Server.

     c. Enter the user name and password of the administrator who has rights on the virtual Administration Server.

4. Click the **Sign in** button.

5. Specify the one-time security code generated by the authenticator app on the mobile device.

   At the first sign-in, configure two-step authentication for your account. If two-factor authentication configuration is not available to you, contact a user who has the Modify object ACLs right in the **General features**: **User permissions** functional area and configured two-factor authentication to add your account to the two-factor authentication allowlist.

6. If forced password change is enabled for your account or your password has expired, the password change window will be displayed. Set a new password to sign-in to Kaspersky Security Center Web Console.

After sign-in, the Kaspersky Security Center Web Console home page is displayed, containing the language and theme that you used last time. You can navigate through Kaspersky Security Center Web Console and use it to work with Kaspersky Security Center Linux.

### Signing out

*To sign out of Kaspersky Security Center Web Console,*

In the upper pane, go to your account menu by clicking your account name, and then select **Sign out**.

Kaspersky Security Center Web Console is closed, and the sign-in page is displayed.

## Kaspersky Security Center Web Console interface

Kaspersky Security Center Linux is managed through the Kaspersky Security Center Web Console interface.

The Kaspersky Security Center Web Console window contains the following items:

- Main menu in the left part of the window
- Upper pane in the upper part of the window
- Work area in the right part of the window

### Main menu

The main menu contains the following sections:

- **Administration Server**. Displays the name of the Administration Server that you are currently connected to. You can open the Administration Server properties by clicking the Administration Server name.
- **Console navigation**. Displays the main menu map. Most of the displayed sections can be added to bookmarks or set as a home page. By default, **Console navigation** is set as a home page. You can change these settings.
- **Monitoring**. Provides an overview of your infrastructure, protection statuses, and statistics.
- **Asset management**. Contains tools for device and hardware management, and Kaspersky application policies.
- **Tasks**. Contains tools for creating and running tasks.

- **Users & Roles**. Allows you to manage users and roles, configure user rights by assigning roles to the users, and associate policy profiles with roles.
- **Repositories**. Provides you access to application repositories.
- **Software management**. Allows you to manage Kaspersky and third-party applications, as well as installation packages and patches.
- **Operations**. Contains a variety of operations, including application licensing, viewing, and managing encrypted drives and encryption events.
- **Discovery & Deployment**. Allows you to poll the network to discover client devices, and distribute the devices to administration groups manually or automatically. This section also contains the quick start wizard and Protection deployment wizard.
- **Marketplace**. Contains information about the entire range of Kaspersky business solutions and allows you to select the ones you need, and then proceed to purchase those solutions at the Kaspersky website.
- **Settings**. Allows you to back up the current state of a web plug-in to be able to restore the saved state later. Contains your personal settings related to the interface appearance, such as interface language or theme.

If necessary, you can minimize the main menu to icons by clicking the chevron sign (<<) at the bottom of the screen.

### Upper pane

The upper pane is always displayed in all console sections and cannot be hidden.

The left side of the pane contains the application name and logo. If you click the application name or logo, the Kaspersky Security Center Web Console home page opens.

On the right side of the pane, the following settings are displayed:

- Notification icon (🔔). If you click the icon, a pane with notifications opens.
- The menu of your account. Contains a link to Kaspersky Security Center Linux Help. It also allows you to sign out of Kaspersky Security Center Linux, change the password for your own account, and view the Kaspersky Security Center Web Console version and the list of installed management web plug-ins.

### Work area

The work area displays the information you choose to view in the sections of the Kaspersky Security Center Web Console interface window. It also contains control elements that you can use to configure how the information is displayed.

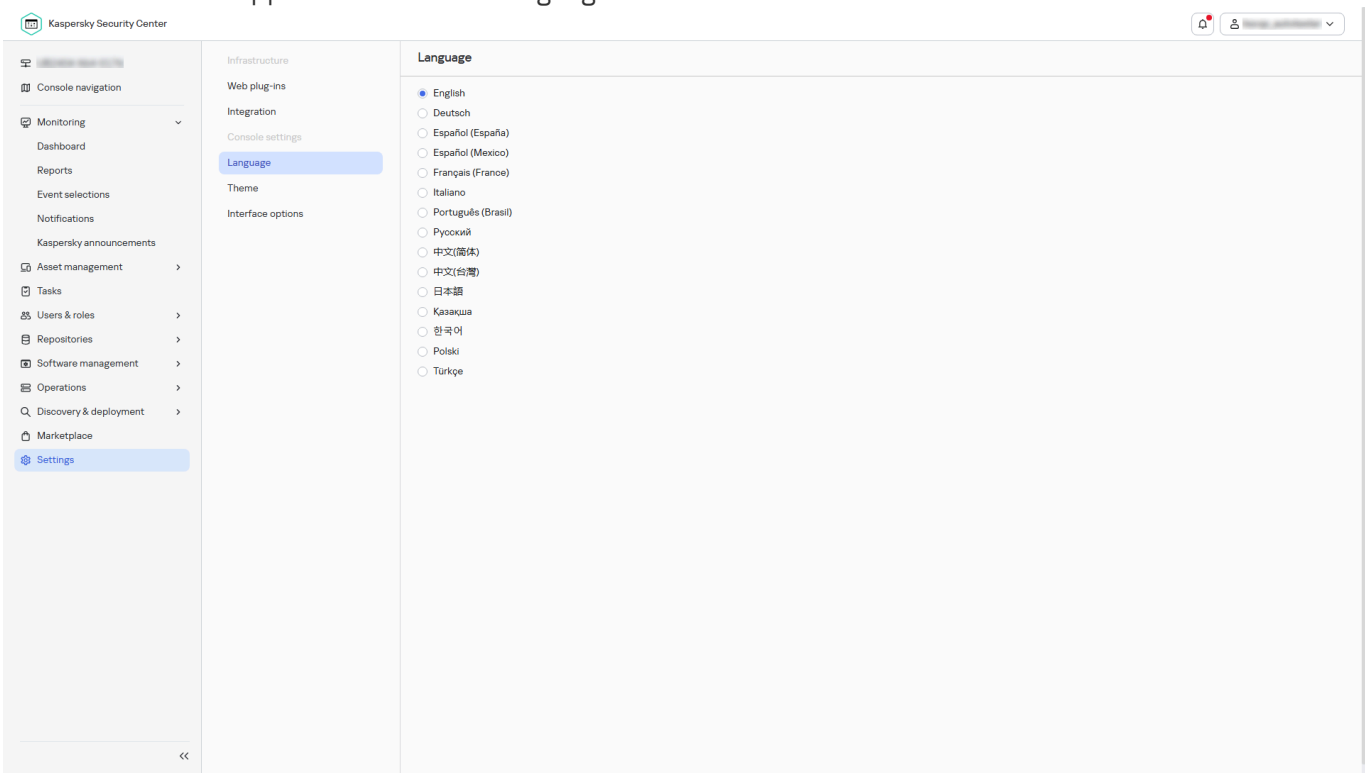
> We recommend to use a single browser tab to work with the Kaspersky Security Center Web Console.

# Changing the language of the Kaspersky Security Center Web Console interface

You can select the language of the Kaspersky Security Center Web Console interface.

*To change the interface language:*

1. In the main menu, go to **Settings** → **Language**.
2. Select one of the supported localization languages.




Changing the language of the Kaspersky Security Center Web Console interface

# Changing the Kaspersky Security Center Web Console home page

The home page is displayed after you sign in to Kaspersky Security Center Web Console.

By default, the **Console navigation section** is set as the home page. If necessary, you can change the home page.

*To change the home page:*

1. In **Console navigation** section, hover the mouse cursor over the item that you want to set as the home page.
2. After the home (⌂) icon is displayed, click the icon.

The home page is changed. A corresponding message is displayed on the screen. The item selected as the home page is marked with the house (⌂) icon.

The **Marketplace** and **Settings** sections cannot be set as the home page.

## Adding and removing bookmarks

You can add frequently used sections of Kaspersky Security Center Web Console to bookmarks to access them quickly from the **Bookmarks** section in the main menu.

If you did not add any section to bookmarks, the **Bookmarks** section is not displayed in the main menu.

You can add to bookmarks only the sections that display pages. For example, if you go to **Asset management** → **Managed devices**, a page with the table of devices opens, which means you can add this section to bookmarks. If a window or no element is displayed after you select the section in the main menu, then you cannot add such a section to bookmarks.

*To add a section to bookmarks:*

1. In the main menu, hover the mouse cursor over the section you want to pin.
2. After the bookmark (🔖) icon is displayed, click the icon.

   The section is displayed in the **Bookmarks** section.

*To remove a section from bookmarks:*

1. In the main menu, go to the **Bookmarks** section.
2. Hover the mouse cursor over the section you want to remove, and then click the bookmark (🔖) icon.

   The section is removed from bookmarks.

You can also add and remove sections from bookmarks in the **Console navigation** section by hovering the mouse cursor over them and clicking the bookmark (🔖) icon. The selected item will be marked with the bookmark (🔖) icon and displayed in the **Bookmarks** section in the main menu. If you want to remove the item from the bookmarks, click the bookmark (🔖) icon.

The **Bookmarks** section is displayed only in the main menu. It is never displayed on the **Console navigation** page.

# Removing Kaspersky Security Center Web Console

You may need to remove Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) in the following cases:

- Restoring data from a backup with another common certificate.
- Reissuing Administration Server common certificate.

- Replacing Web Console certificate with custom certificate.
- Kaspersky Security Center Web Console in no longer used on a device.

*To remove Kaspersky Security Center Web Console:*

1. Depending on your Linux distribution, run one of the following commands:
   - `sudo dnf remove ksc-web-console`
   - `sudo apt remove ksc-web-console`
2. Check the result by executing the following command:

   `sudo systemctl status KSC*`

   Kaspersky Security Center Web Console must be absent in the command output.

If you want to restore Kaspersky Security Center Web Console, install it on the device as described in the article: Installing Kaspersky Security Center Web Console.

# Quick start wizard

Kaspersky Security Center Linux allows you to adjust a minimum selection of settings required to build a centralized management system for protecting your network against security threats. This configuration is performed through the quick start wizard. When the wizard is running, you can make the following changes to the application:

- Add key files or enter activation codes that can be automatically distributed to devices within administration groups.
- Set up email delivery of notifications of events that occur during operation of Administration Server and managed applications.
- Create a protection policy for workstations and servers, as well as malware scan tasks, update download tasks, and data backup tasks, for the top level of the hierarchy of managed devices.

  The quick start wizard creates policies only for those applications whose **Managed devices** folder does not contain policies. The quick start wizard does not create tasks if tasks with the same names have already been created for the top level in the hierarchy of managed devices.

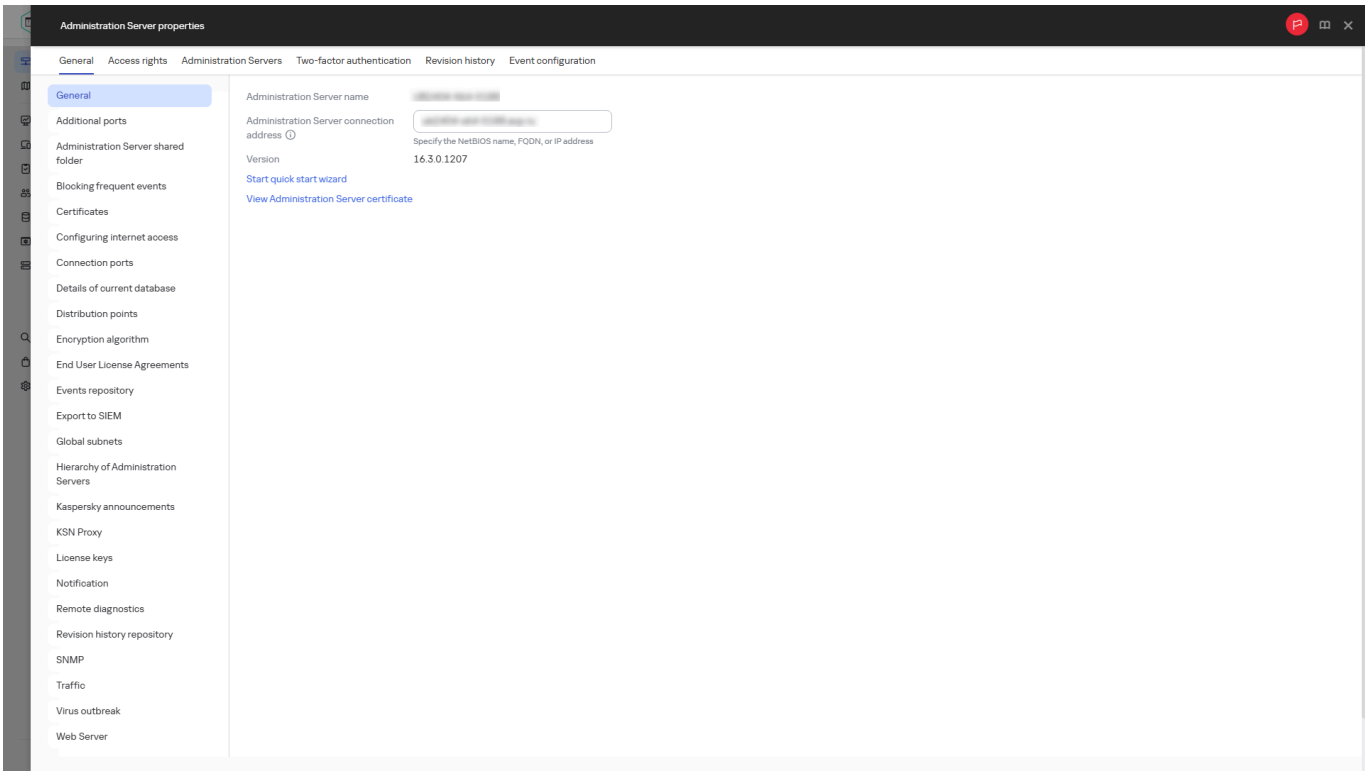
The application automatically prompts you to run the quick start wizard after Administration Server installation, at the first connection to it. You can also start the quick start wizard manually at any time.

*To start the quick start wizard manually:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **General** section.




Administration Server properties window

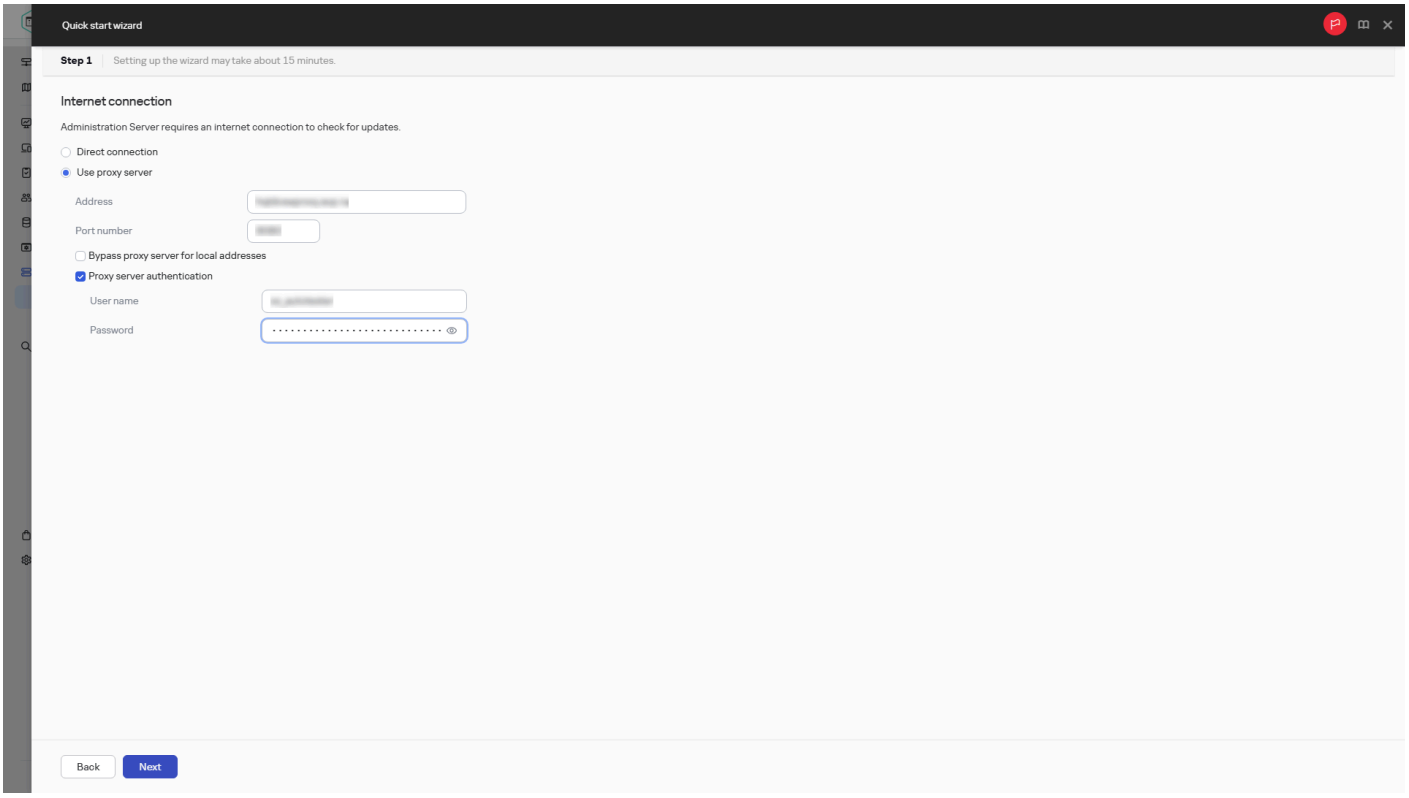
3. Click **Start quick start wizard**.

The wizard prompts you to perform initial configuration of the Administration Server. Follow the steps of the wizard. Proceed through the wizard by using the **Next** button.

# Step 1. Specifying the internet connection settings

Specify the internet access settings for Administration Server. You must configure internet access to use Kaspersky Security Network and to download updates of anti-virus databases for Kaspersky Security Center Linux and managed Kaspersky applications.

Enable the **Use proxy server** option if you want to use a proxy server when connecting to the internet. If this option is enabled, the fields are available for entering settings. Specify the following settings for a proxy server connection:




Internet connection settings

- **Address**

  Address of the proxy server used for Kaspersky Security Center Linux connection to the internet.

- **Port number**

  Number of the port through which Kaspersky Security Center Linux proxy connection will be established.

- **Bypass proxy server for local addresses**

  No proxy server will be used to connect to devices in the local network.

- **Proxy server authentication**

  If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

  This entry field is available if the **Use proxy server** check box is selected.

- **User name**

  User account under which connection to the proxy server is established (this field is available if the **Proxy server authentication** check box is selected).

- **Password**

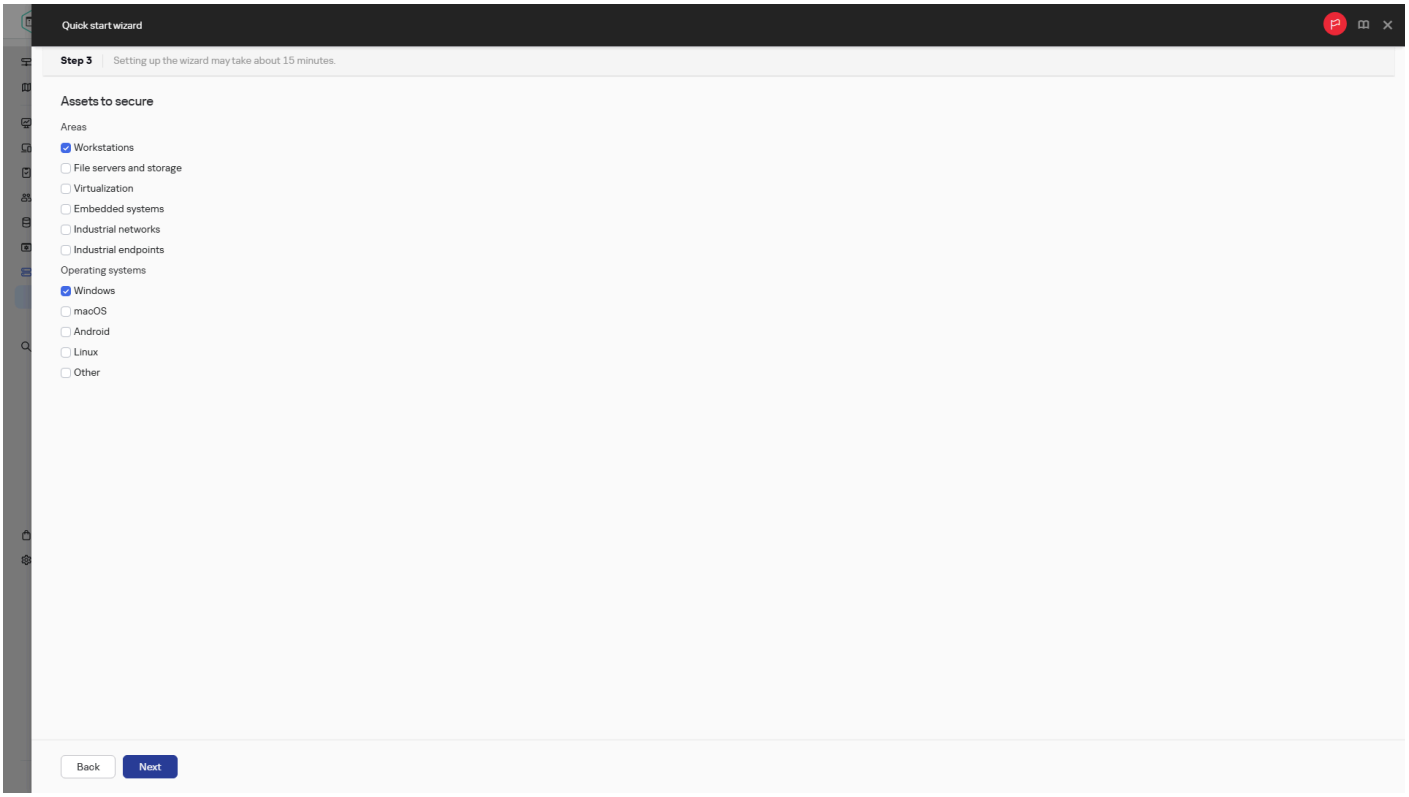
  Password set by the user under whose account the proxy server connection is established (this field is available if the **Proxy server authentication** check box is selected).

  To see the entered password, click and hold the **Show** button for as long as you require.

You can configure internet access later, separately from the quick start wizard.

# Step 2. Downloading required updates

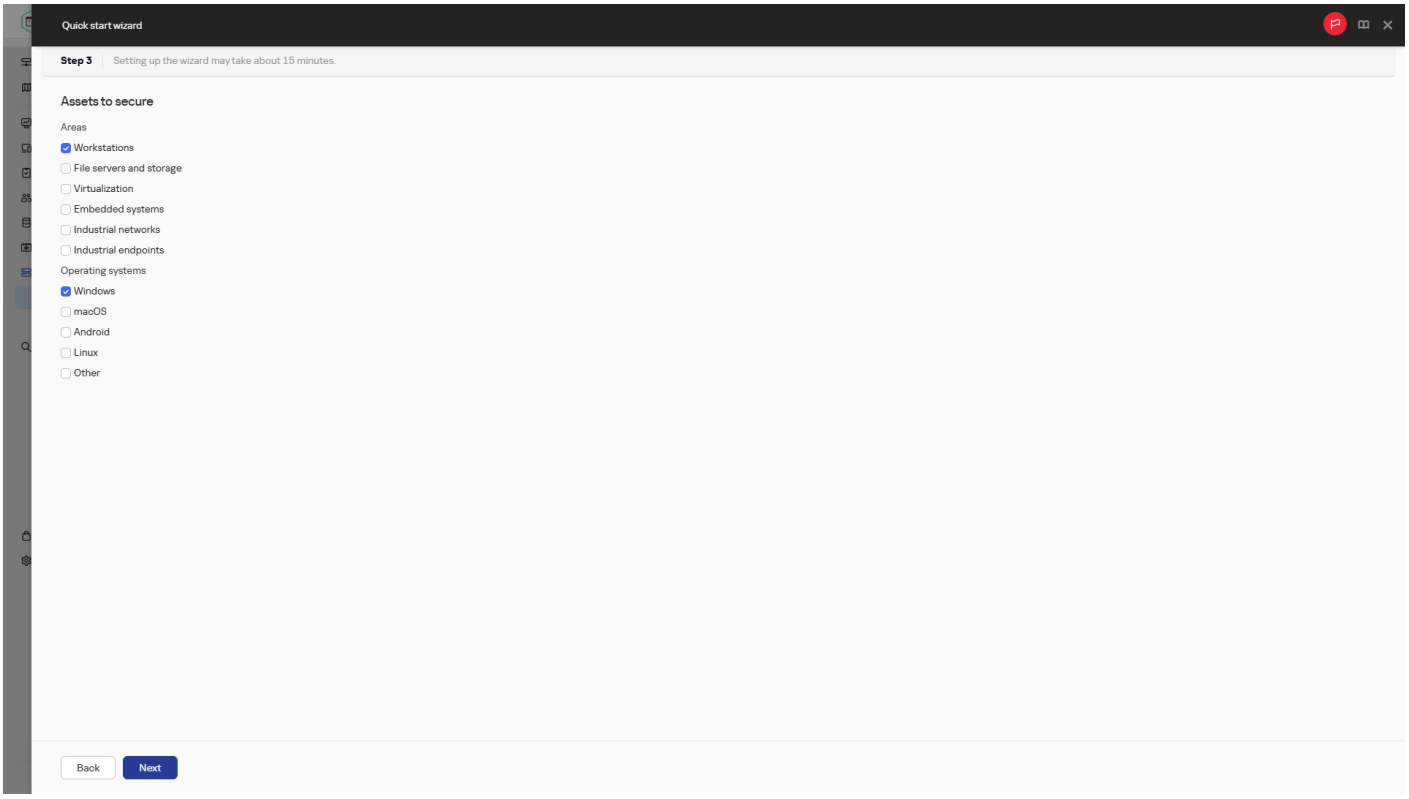
The required updates are downloaded from the Kaspersky servers automatically.




Downloading required updates

# Step 3. Selecting the assets to secure

Select the protection areas and operating systems that are in use on your network. When you select these options, you specify the filters for application management plug-ins and distribution packages on Kaspersky servers that you can download to install on client devices on your network.




Selecting the assets to secure

Select the options:

- **Areas**

  You can select the following protection scopes:

  - **Workstations**
  - **File servers and storage**
  - **Virtualization**
  - **Embedded systems**
  - **Industrial networks**
  - **Industrial endpoints**

- **Operating systems**

  You can select the following platforms:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Other

  For information about supported operating systems, refer to Hardware and software requirements for Kaspersky Security Center Web Console.

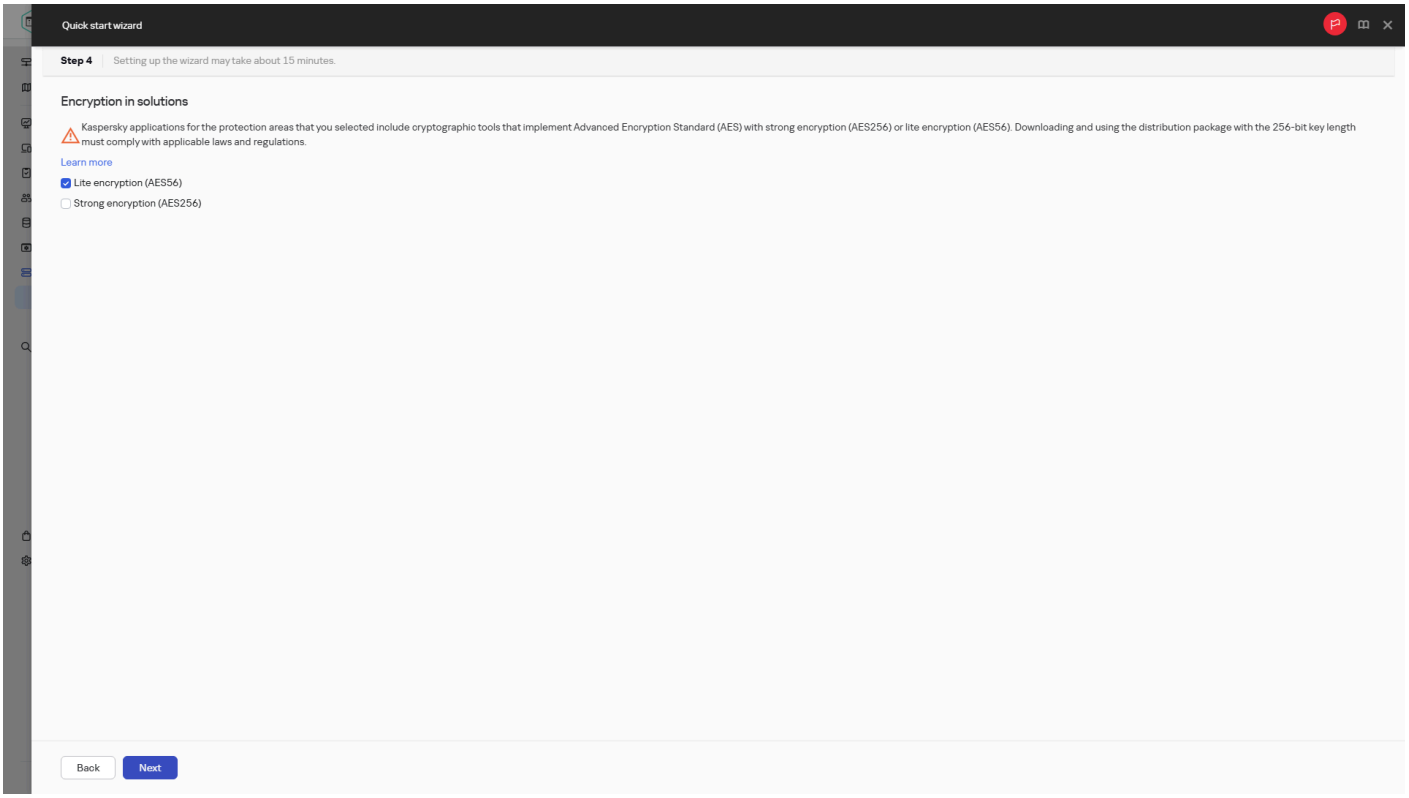
You can select the Kaspersky application packages from the list of available packages later, separately from the quick start wizard. To simplify the search for the required packages, you can filter the list of available packages by various criteria.

# Step 4. Selecting encryption in solutions

The **Encryption in solutions** window is displayed only if you have selected **Workstations** as a protection scope.

Kaspersky Endpoint Security for Windows includes encryption tools for information stored on Windows-based client devices. These encryption tools have the Advanced Encryption Standard (AES) implemented with a 256-bit or 56-bit key length.

Download and usage of the distribution package with a 256-bit key length must be performed in compliance with applicable laws and regulations. To download a distribution package of Kaspersky Endpoint Security for Windows that is valid for the needs of your organization, consult the legislation of the country where the client devices of your organization are located.




Selecting encryption in solutions

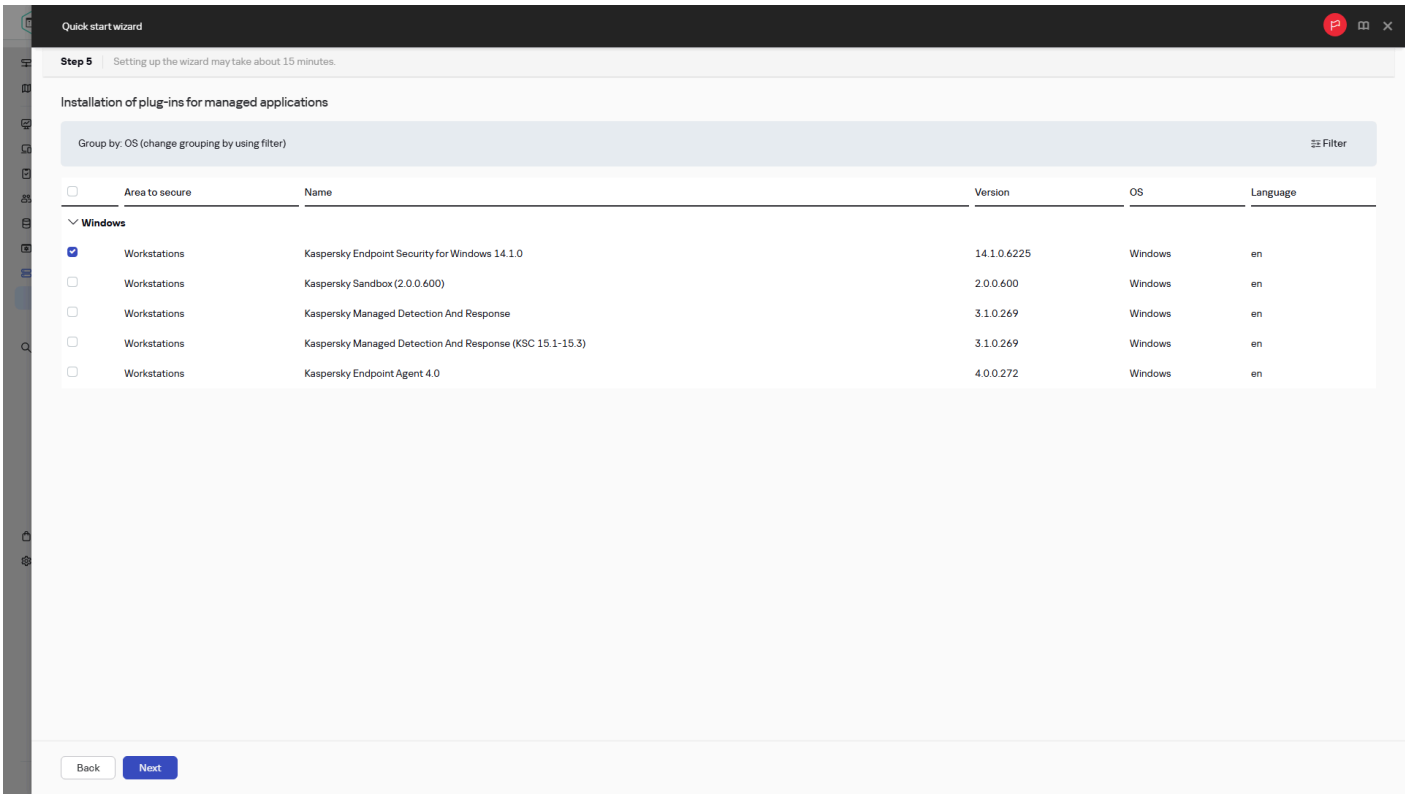
In the **Encryption in solutions** window, select one of the following encryption types:

- Lite encryption. This encryption type uses a 56-bit key length.
- Strong encryption. This encryption type uses a 256-bit key length.

You can select the distribution package for Kaspersky Endpoint Security for Windows with the required encryption type later, separately from the quick start wizard.

# Step 5. Configuring installation of plug-ins for managed applications

Select plug-ins for managed applications to install. A list of plug-ins located on Kaspersky servers is displayed. The list is filtered according to the options selected on the previous step of the wizard. By default, a full list includes plug-ins of all languages. To display only plug-in of specific language, use filter.




Installation of plug-ins for managed applications

The list of plug-ins includes the following columns:

- **Area to secure**

  The selected areas to secure are displayed in this column.

- **Type**

  The plug-in types are displayed in this column.

- **Name**

  The plug-ins depending of the protection areas and platforms that you have selected on the previous step are selected.

- **Version**

  The list includes plug-ins of all the versions placed on Kaspersky servers. By default, the plug-ins of the latest versions are selected.

- **Latest version**

  This column indicates whether a plug-in version is the latest. If **true** value is displayed, the corresponding plug-in is of the latest version. If **false** value is displayed, the corresponding plug-in has a later version.

- **OS**

  This column displays plug-ins operating systems.

- **Language**

  By default, the localization language of a plug-in is defined by the Kaspersky Security Center Linux language that you have selected at installation. You can specify other languages in **Show the Administration Console localization language or** drop-down list.

After the plug-ins are selected, click **Next** to start installation.

You can install management plug-ins for Kaspersky applications manually, separately from the quick start wizard.

The quick start wizard automatically installs the selected plug-ins. To install some plug-ins, you must accept the terms of the EULA. Read the text of EULA displayed, select the **I agree to participate in Kaspersky Security Network** check box and click the **Install** button. If you do not accept the terms of the EULA, the plug-in is not installed.

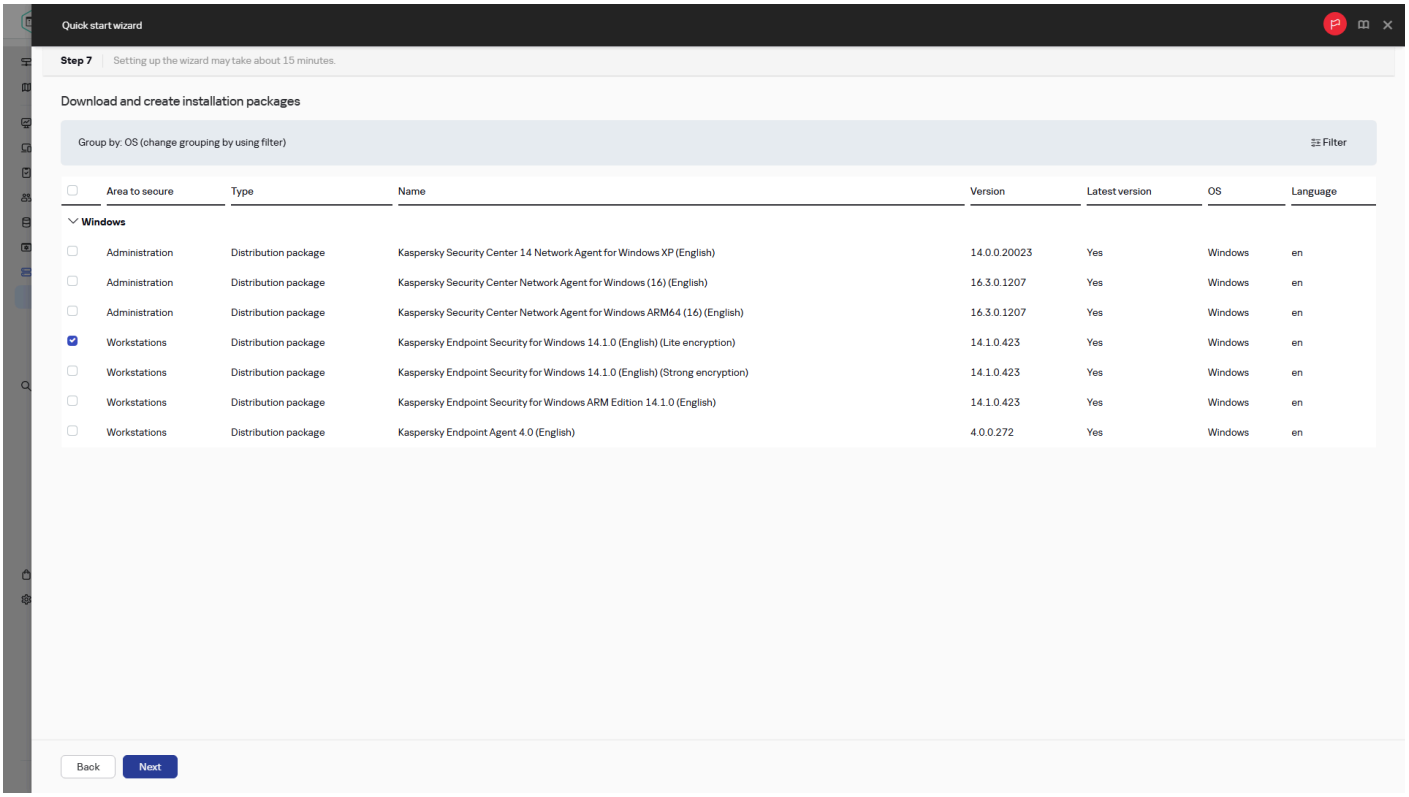
When all the selected plug-ins are installed, the quick start wizard automatically takes you to the next step.

# Step 6. Downloading distribution packages and creating installation packages

Select the distribution packages to download.

Distributives of managed applications may require a specific minimum version of Kaspersky Security Center Linux to be installed.

After you have selected an encryption type for Kaspersky Endpoint Security for Windows, a list of distribution packages of both encryption types is displayed. A distribution package with the selected encryption type is selected in the list. You can select distribution packages of any encryption type. The distribution package language corresponds to the Kaspersky Security Center Linux language. If an application distribution package for the Kaspersky Security Center Linux language does not exist, the English distribution package is selected.



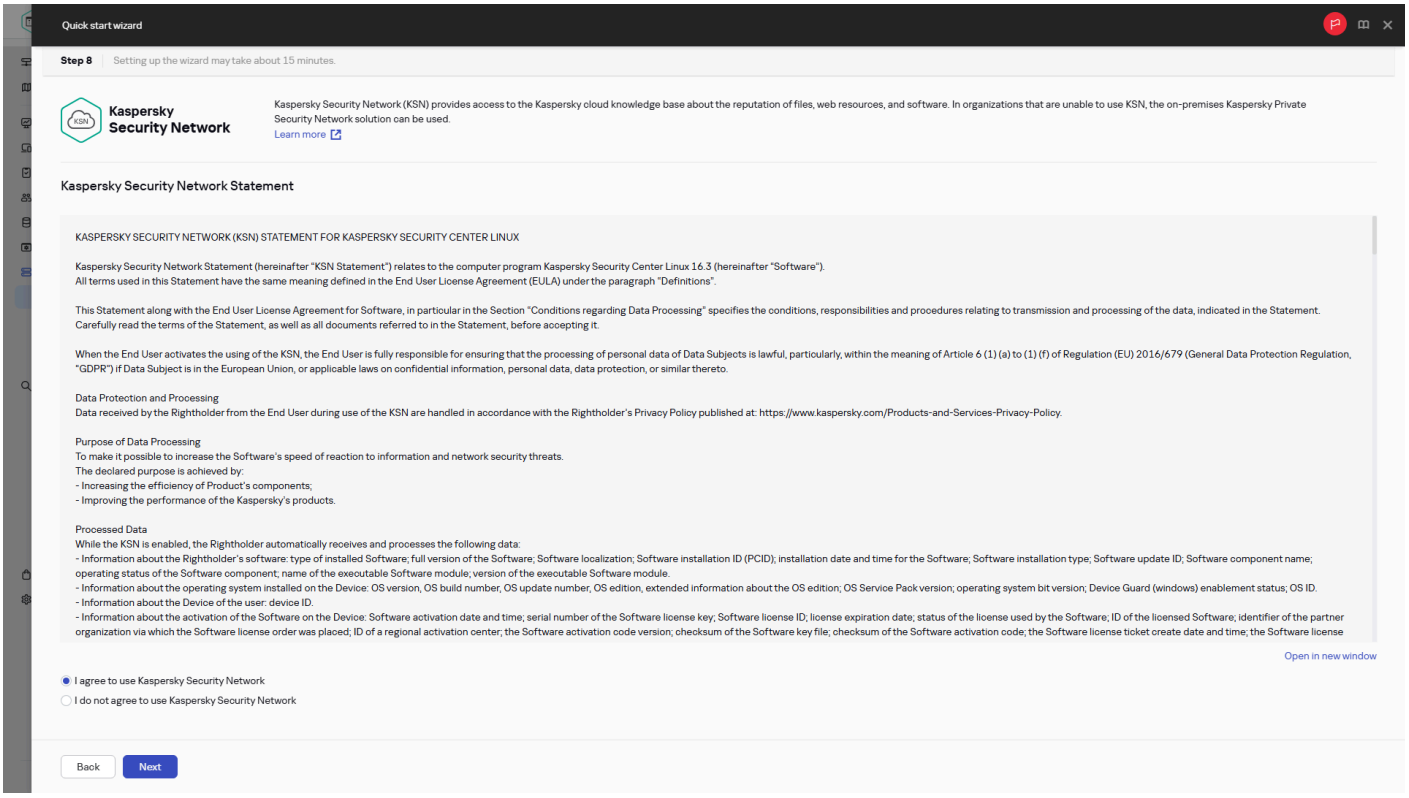

Downloading distribution packages and creating installation packages

To finish downloading of some distribution packages you must accept EULA. When you click the **Accept** button, the text of EULA is displayed. To proceed to the next step of the wizard, you must accept the terms and conditions of the EULA and the terms and conditions of Kaspersky Privacy Policy. If you do not accept the terms and conditions, the downloading of the package is canceled.

After you have accepted the terms and conditions of the EULA and the terms and conditions of Kaspersky Privacy Policy, the downloading of the distribution packages continues. Later, you can use installation packages to deploy Kaspersky applications on client devices.

# Step 7. Configuring Kaspersky Security Network

Specify the settings for relaying information about Kaspersky Security Center Linux operations to the Kaspersky Security Network knowledge base.




Configuring Kaspersky Security Network

Choose one of the following options:

- **I agree to participate in Kaspersky Security Network**

  Kaspersky Security Center Linux and managed applications installed on client devices will automatically transfer their operation details to Kaspersky Security Network. Participation in Kaspersky Security Network ensures faster updates of databases containing information about viruses and other threats, which ensures a faster response to emergent security threats.

- **I do not agree to participate in Kaspersky Security Network**

  Kaspersky Security Center Linux and managed applications will provide no information to Kaspersky Security Network.

  If you select this option, the use of Kaspersky Security Network will be disabled.

You can set up access to Kaspersky Security Network (KSN) later, separately from the quick start wizard.

# Step 8. Selecting the application activation method

Select one of the following Kaspersky Security Center Linux activation options:

- **By entering your activation code**

  An *activation code* is a unique sequence of twenty Latin letters and numerals. You enter an activation code to add a key that activates Kaspersky Security Center Linux. You receive the activation code through the email address that you specified after purchasing Kaspersky Security Center.

  To activate the application by using the activation code, you need internet access in order to connect to Kaspersky activation servers.

  If you have selected this activation option, you can enable the **Automatically deploy license key to managed devices** option.

  If this option is enabled, the license key will be deployed automatically to managed devices.

  If this option is disabled, you can deploy license key to managed devices later in the **Operations** → **Licensing** → **Licenses** section of the main menu.

- **By specifying a key file**

  *Key file* is a file with the key extension provided to you by Kaspersky. A key file is intended for adding a key that activates the application.

  You receive your key file through the email address that you specified after purchasing Kaspersky Security Center.

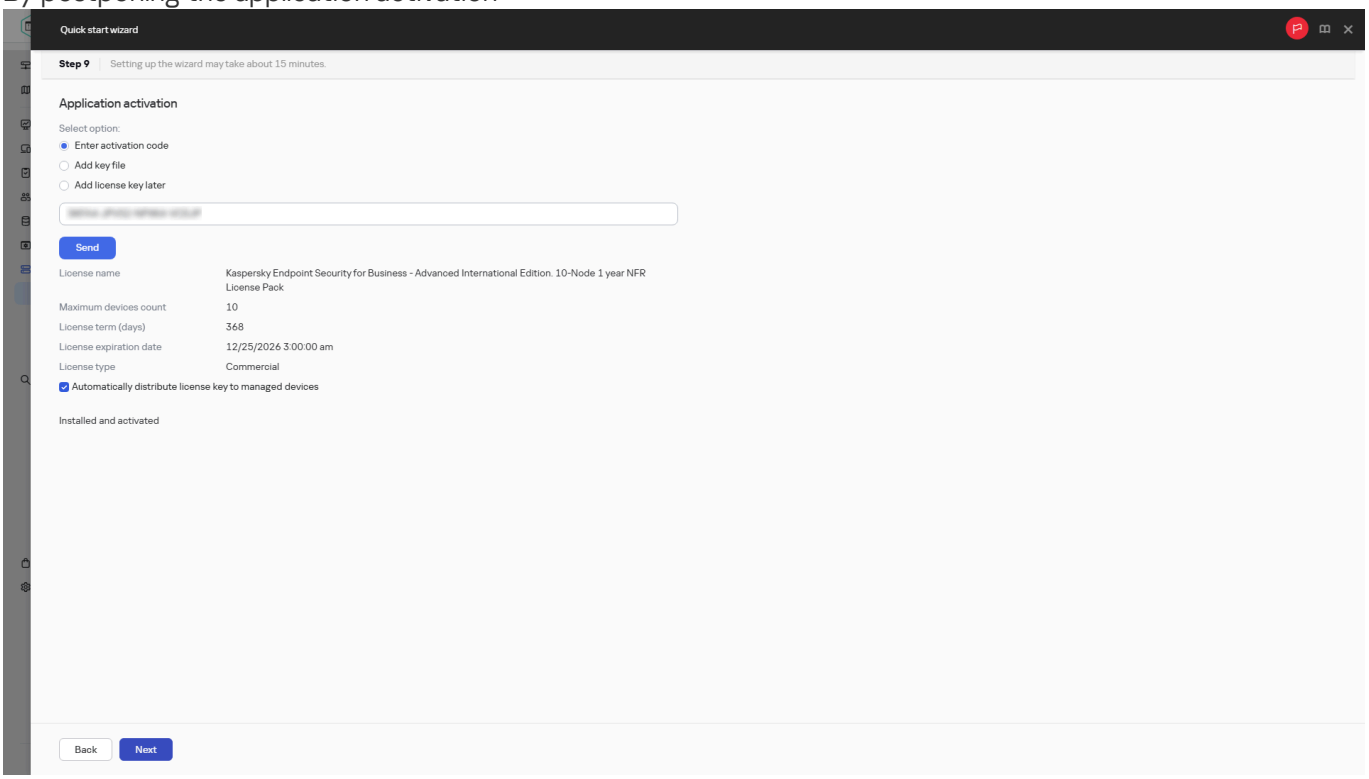
  You do not need to connect to Kaspersky activation servers in order to activate the application with a key file.

  If you have selected this activation option, you can enable the **Automatically deploy license key to managed devices** option.

  If this option is enabled, the license key will be deployed automatically to managed devices.

  If this option is disabled, you can deploy license key to managed devices later in the **Operations** → **Licensing** → **Licenses** section of the main menu.

- By postponing the application activation



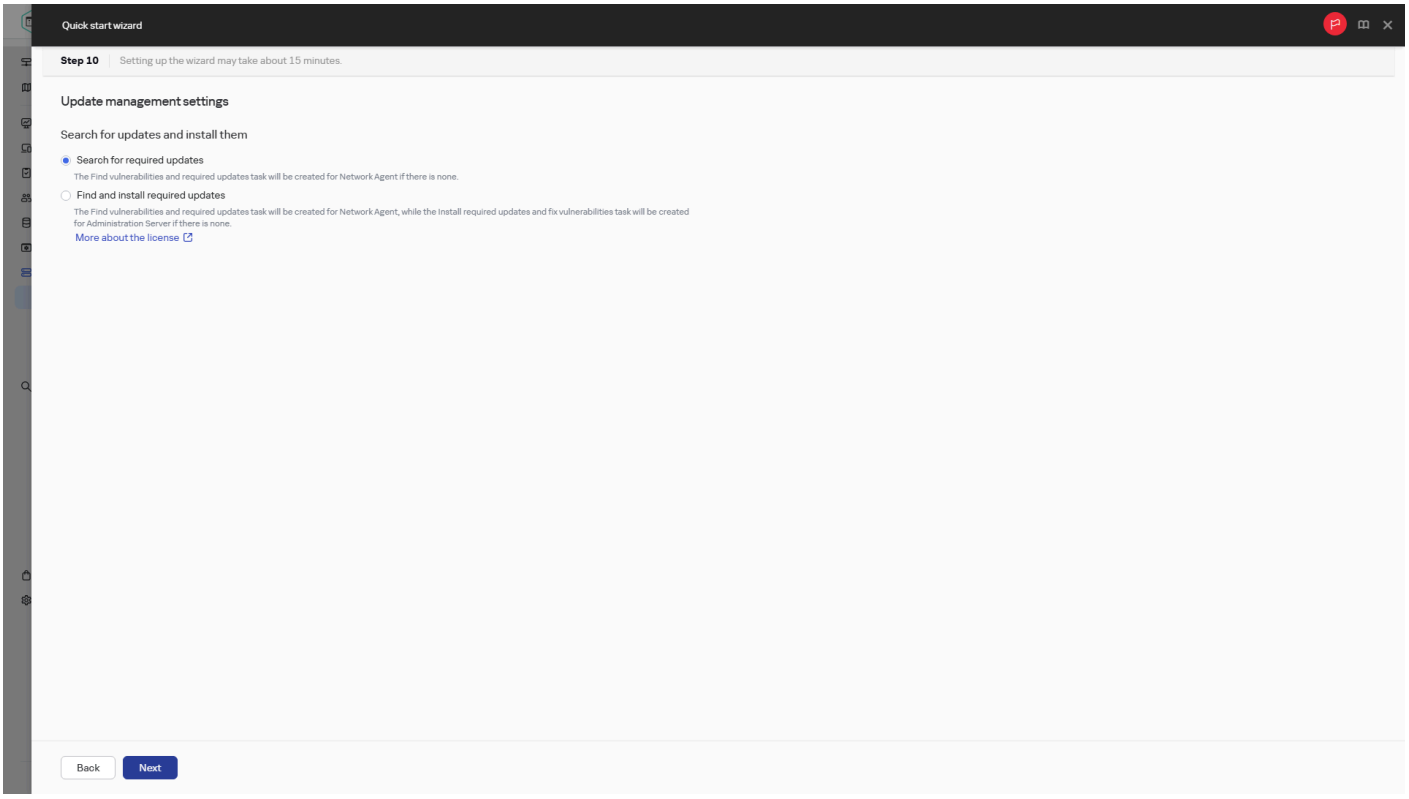

Selecting the application activation method

If you chose to postpone application activation, you can add a license key later at any time by selecting **Operations → Licensing**.

When working with Kaspersky Security Center deployed from a paid AMI or for a usage-based monthly billed SKU, you cannot specify a key file or enter a code.

# Step 9. Specifying the third-party update management settings

The **Update management settings** step of the quick start wizard is not displayed if you do not have the Vulnerability and patch management license and the *Find vulnerabilities and required updates* task already exists.




Third-party update management settings

For third-party software updates, select one of the following options:

- **Search for required updates**

  The *Find vulnerabilities and required updates* task is created automatically, if you do not have one.

  This option is selected by default.

- **Find and install required updates**

  The *Find vulnerabilities and required updates* and *Install required updates and fix vulnerabilities* tasks are created automatically, if you do not have ones.

  This option is only available under the Vulnerability and patch management license.

For Windows Update updates, select **Use the update sources defined in the domain policy.**

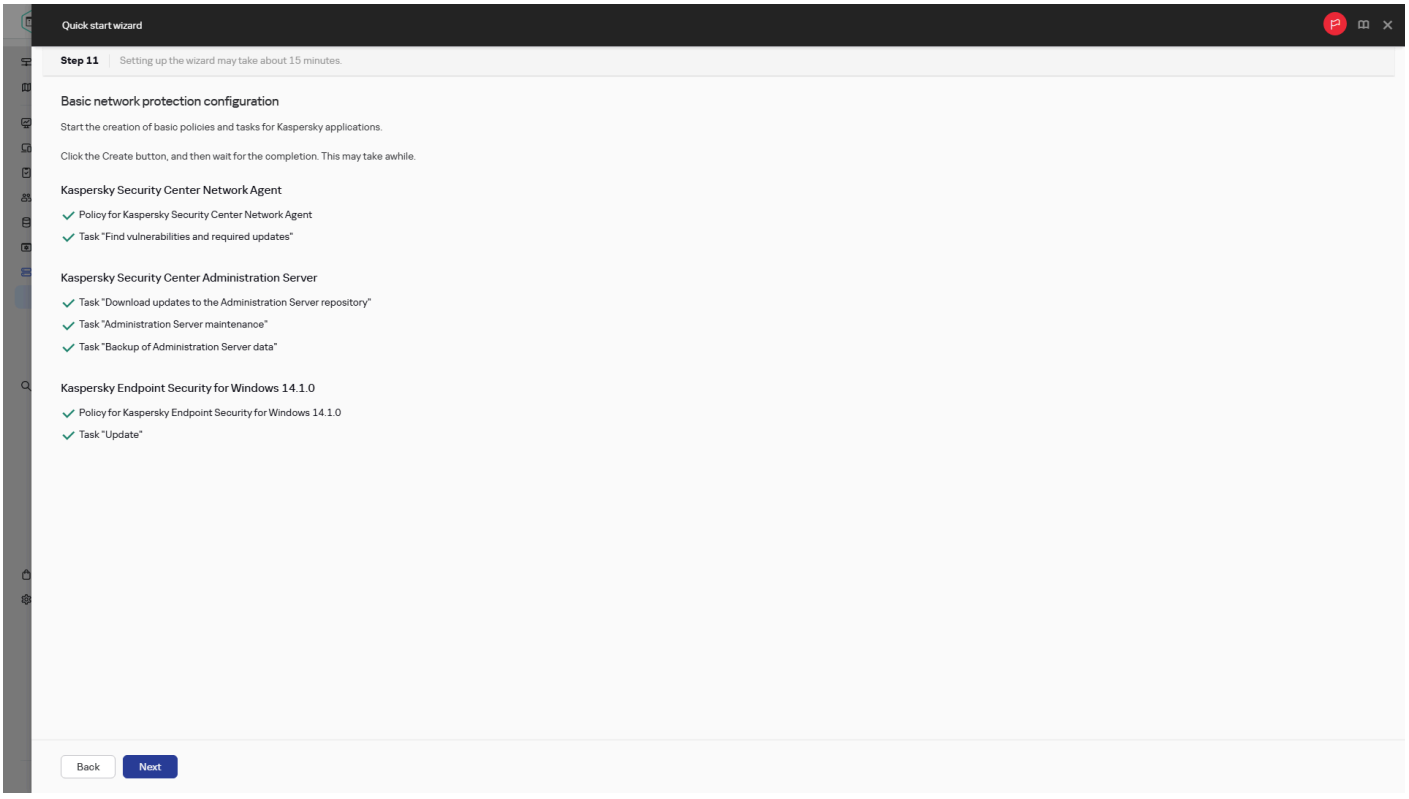
Client devices will download Windows Update updates according to your domain policy settings. Network Agent policy is created automatically, if you do not have one.

You can create the *Find vulnerabilities and required updates* and *Install required updates and fix vulnerabilities* tasks separately from the quick start wizard.

# Step 10. Creating a basic network protection configuration

You can check a list of policies and tasks that are created.

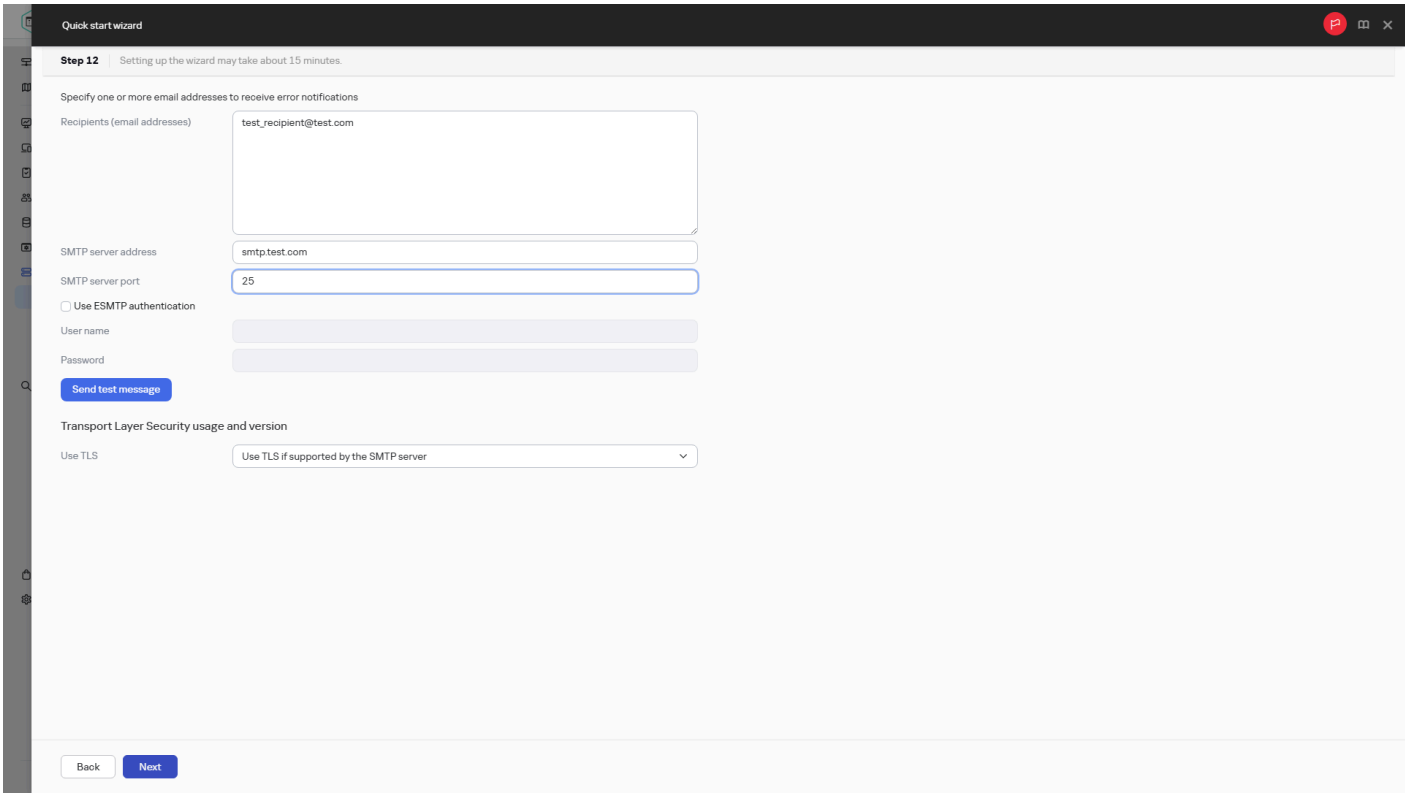
Wait for the creation of policies and tasks to complete before proceeding to the next step of the wizard.




Creating a basic network protection configuration

# Step 11. Configuring email notifications

Configure the delivery of notifications about events registered during the operation of Kaspersky applications on client devices. These settings will be used as the default settings for application policies.




Configuring email notifications

To configure the delivery of notifications about events occurring in Kaspersky applications, use the following settings:

- **Recipients (email addresses)**

  The email addresses of users to whom the application will send notifications. You can specify one or more addresses. If you enter more than one address, separate them with a semicolon.

- **SMTP server address**

  The address or addresses of your organization's mail servers.

  If you enter more than one address, separate them with a semicolon. You can use the following values:

  - IPv4 or IPv6 address
  - DNS name of the SMTP server

- **SMTP server port**

  Communication port number of the SMTP server. If you use several SMTP servers, the connection to them is established through the specified communication port. The default port number is 25.

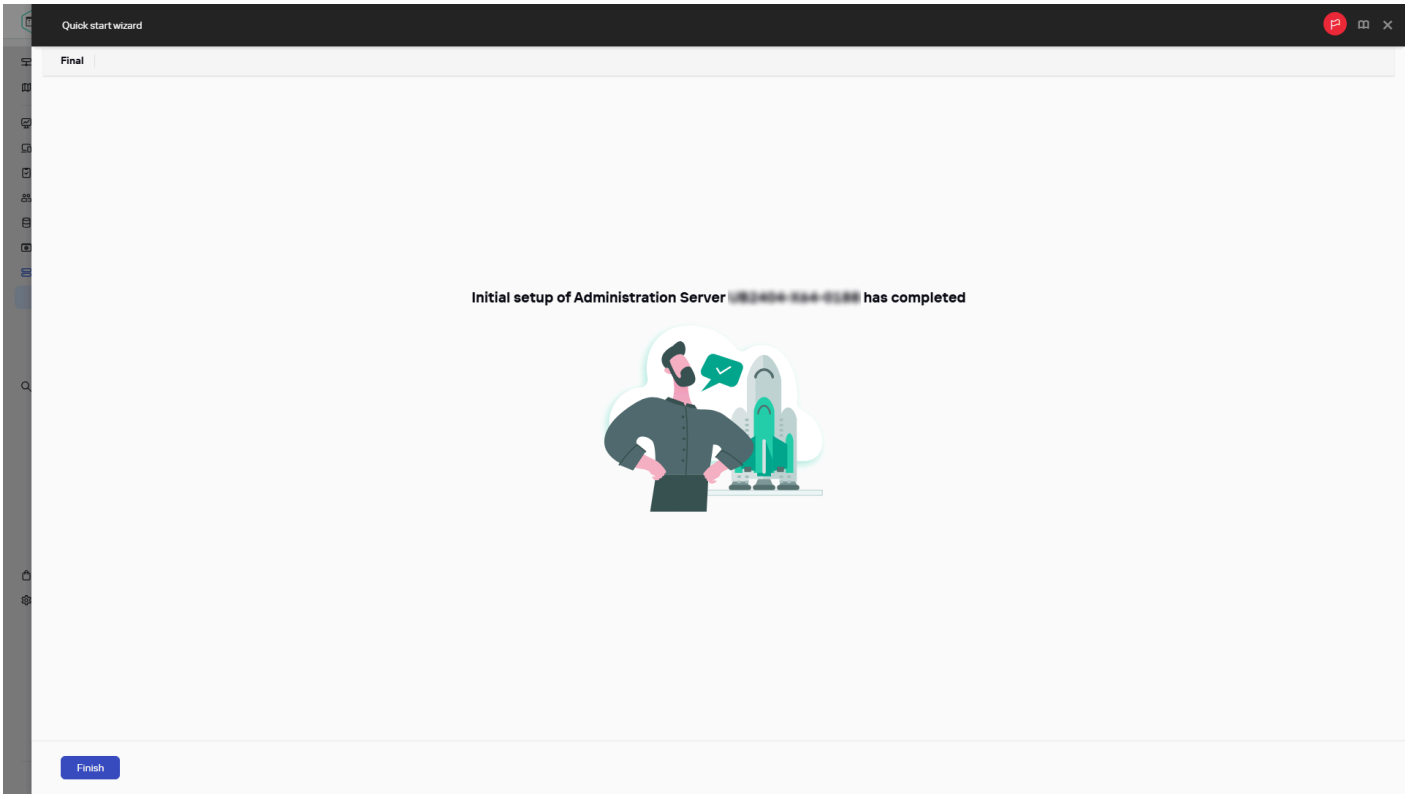
- **Use ESMTP authentication**

  Enables support of ESMTP authentication. When the check box is selected, in the **User name** and **Password** fields you can specify the ESMTP authentication settings. This check box is cleared by default.

You can test the new email notification settings by clicking the **Send test message** button.

## Step 12. Closing the quick start wizard

To close the wizard, click the **Finish** button.




Final step of Quick start wizard

After you have completed the quick start wizard, you can run the Protection deployment wizard to automatically install anti-virus applications or Network Agent on devices on your network.

# Protection deployment wizard

To install Kaspersky applications, you can use the Protection deployment wizard. The Protection deployment wizard enables remote installation of applications either through specially created installation packages or directly from a distribution package.

The Protection deployment wizard performs the following actions:

- Downloads an installation package for application installation (if it was not created earlier). The installation package is located at **Software management** → **Installation packages**. You can use this installation package for the application installation in the future.
- Creates and runs a remote installation task for specific devices or for an administration group. The newly created remote installation task is stored in the **Tasks** section. You can later start this task manually. The task type is **Install application remotely**.

If you want to install Network Agent on devices with the SUSE Linux Enterprise Server 15 operating system, install the insserv-compat package first to configure Network Agent.

## Step 1. Starting Protection deployment wizard

You can start the Protection deployment wizard manually at any time.

*To start the Protection deployment wizard manually,*

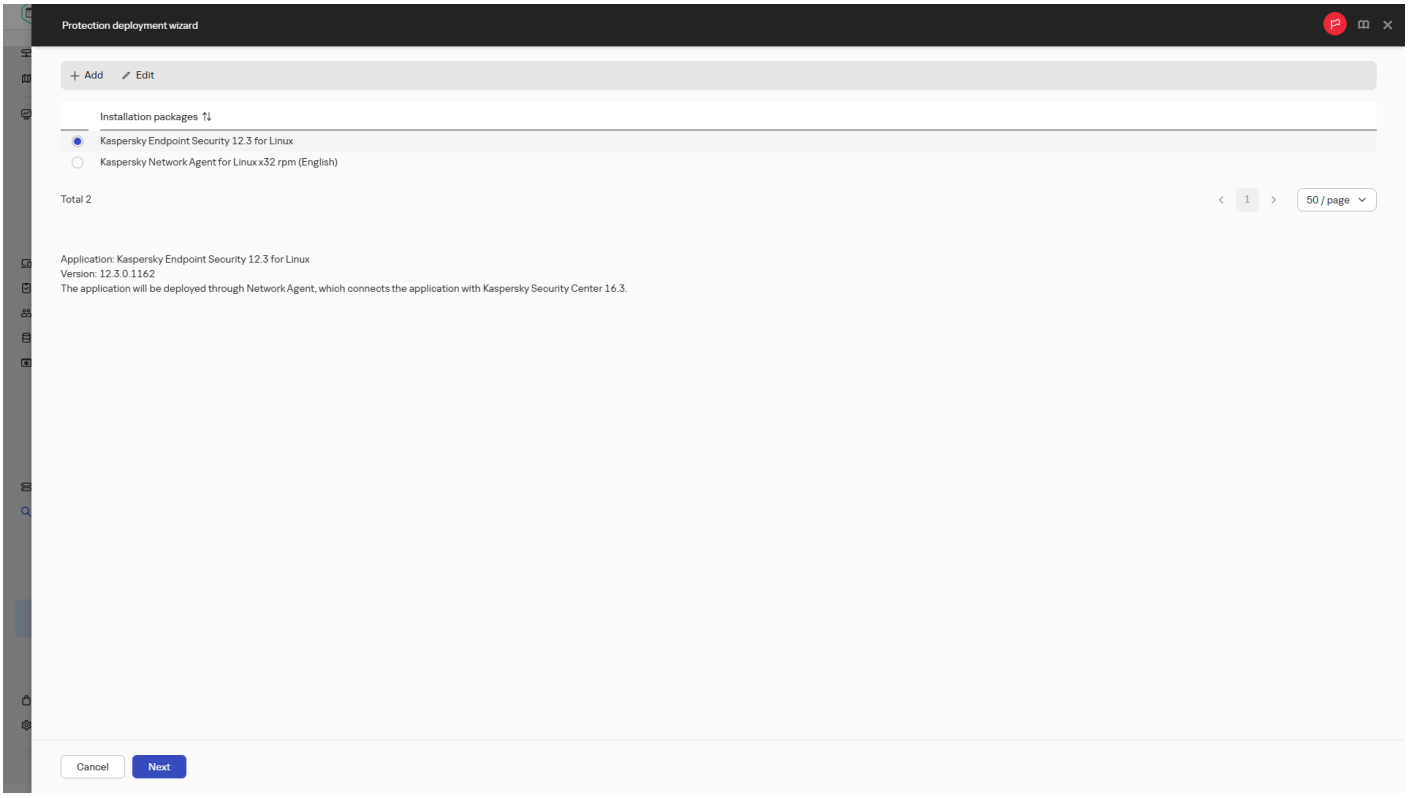
In the main menu, go to **Discovery & deployment** → **Deployment & assignment** → **Protection deployment wizard**.

The Protection deployment wizard starts. Proceed through the wizard by using the **Next** button.

## Step 2. Selecting the installation package

Select the installation package of the application that you want to install.

If the installation package of the required application is not listed, click the **Add** button and then select the application from the list.




Selecting the installation package

# Step 3. Selecting a method for distribution of key file or activation code

Select a method for the distribution of the key file or the activation code:

- **Do not add license key to installation package**

  The key is automatically distributed to all devices with which it is compatible:

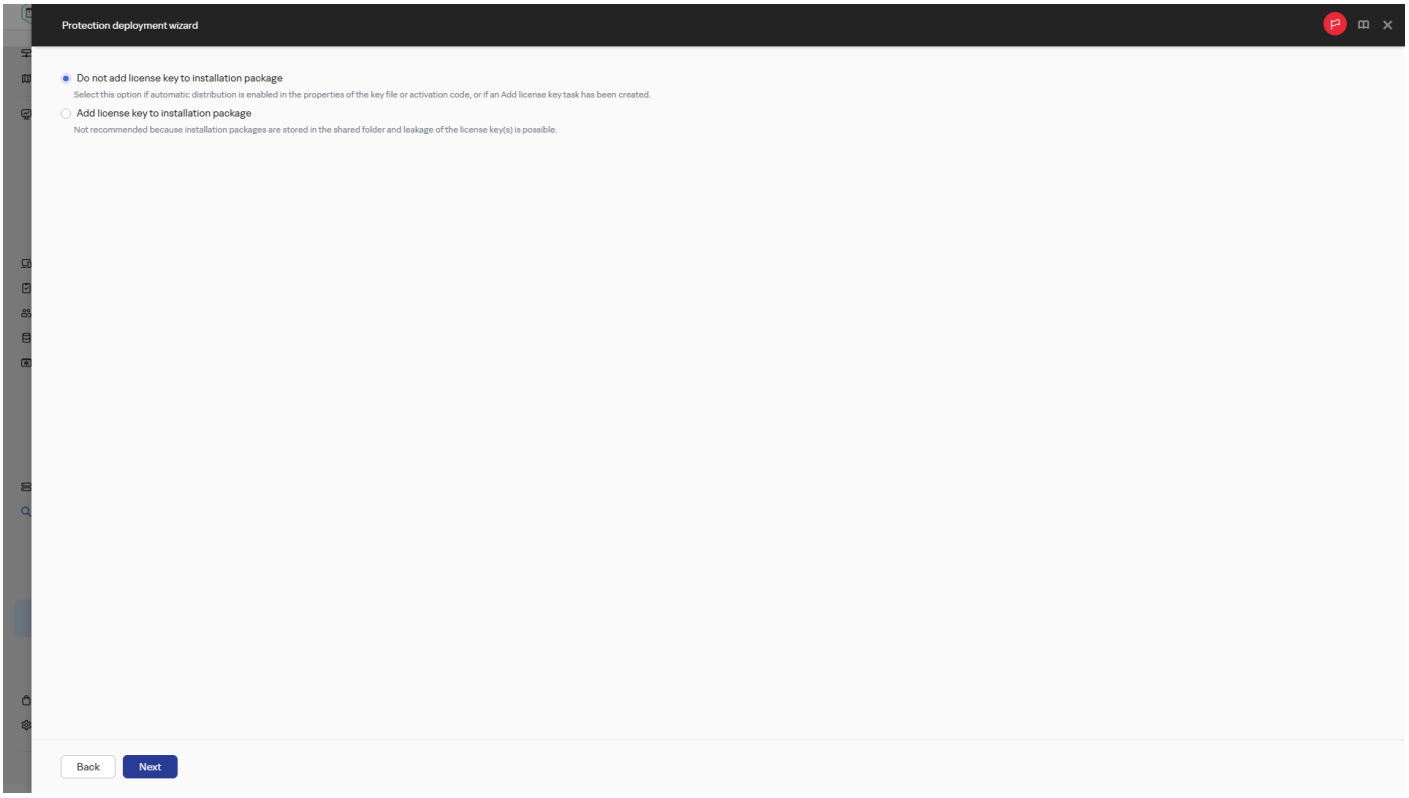
  - If automatic distribution has been enabled in the key properties.
  - If the **Add key** task has been created.

- **Add license key to installation package**

  The key is distributed to devices together with the installation package.

  > We do not recommend that you distribute the key using this method because the shared Read access rights are enabled to the repository of installation packages.

If the installation package already includes a key file or an activation code, this window is displayed, but it only contains the license key information.

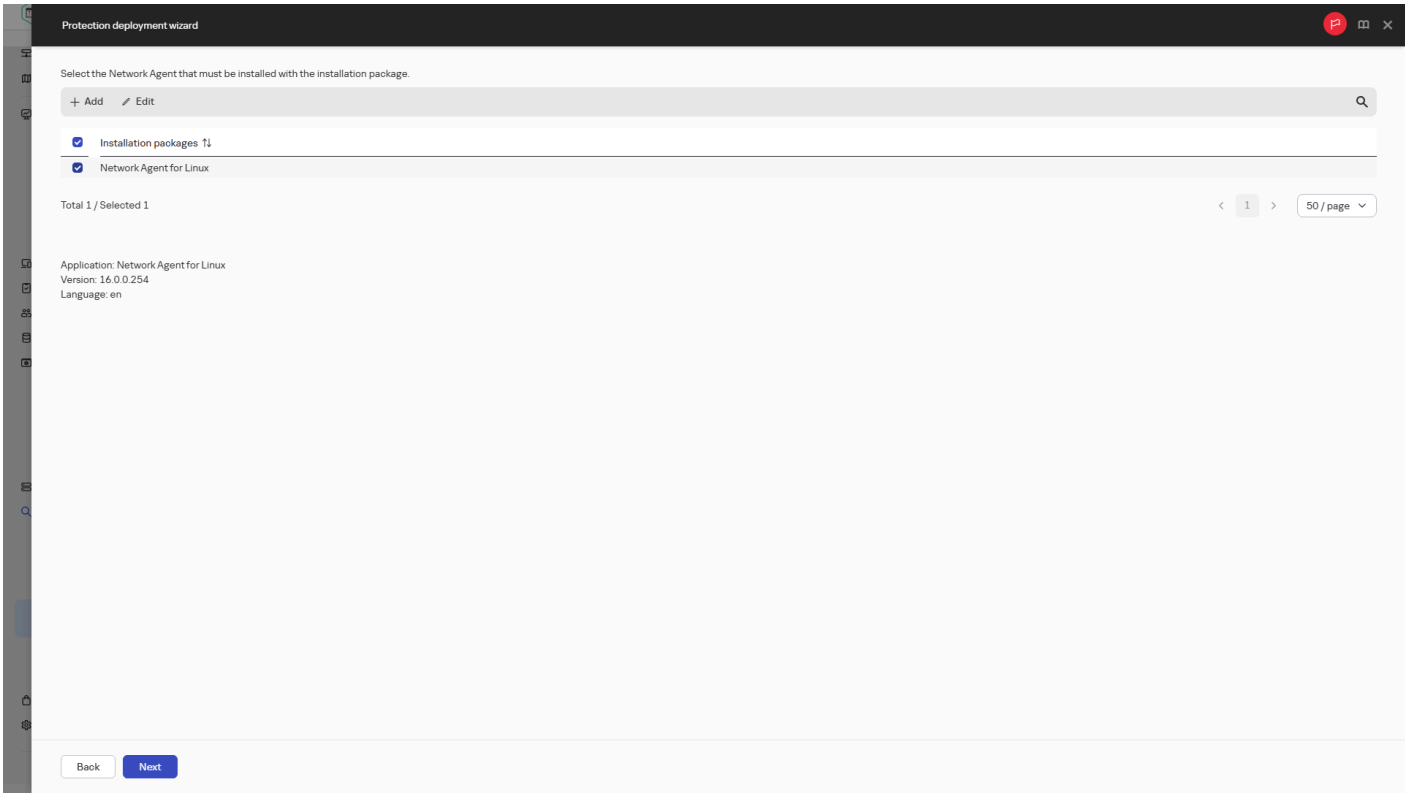



Selecting a method for distribution of key file or activation code

# Step 4. Selecting the Network Agent version

If you selected the installation package of an application other than Network Agent, you also have to install Network Agent, which connects the application with Administration Server.

Select the latest version of Network Agent.




Selecting the Network Agent version

# Step 5. Selecting devices

Specify a list of devices on which the application will be installed:

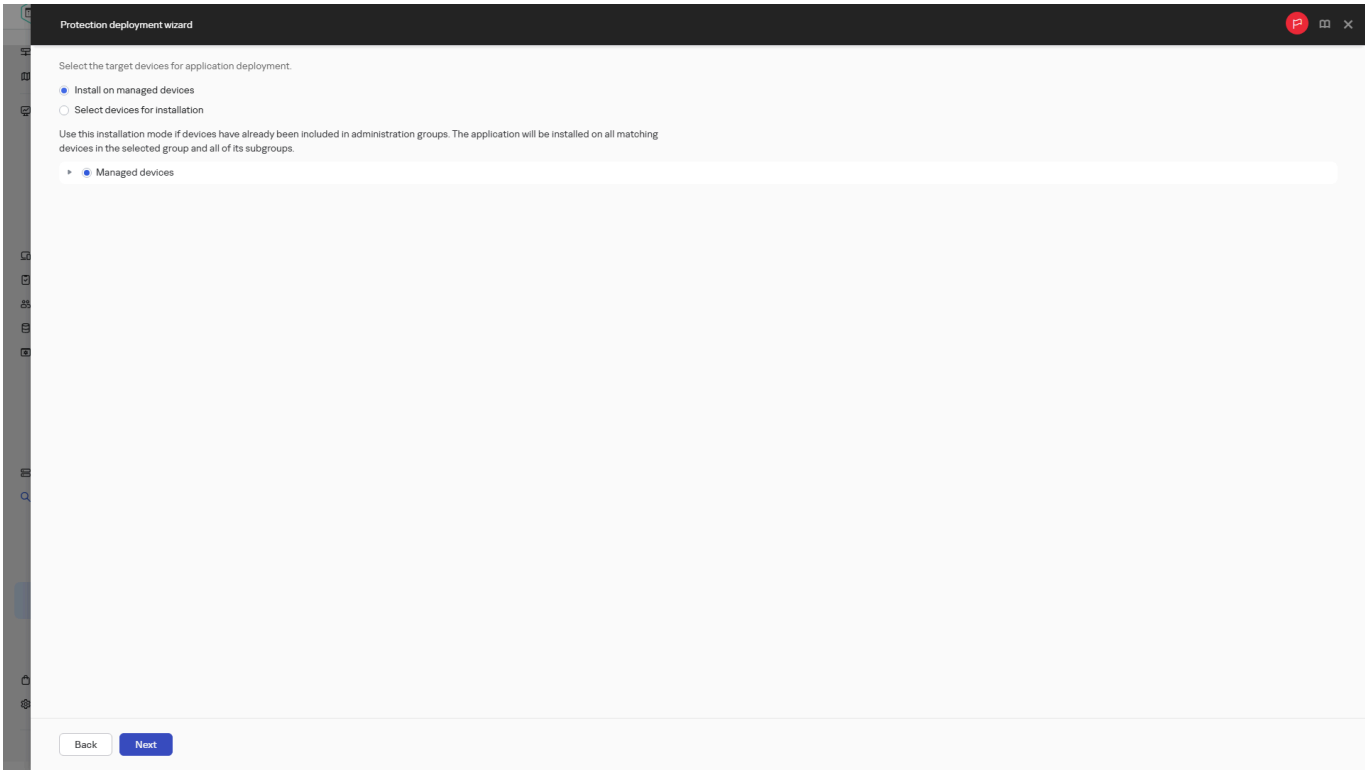
- **Install on managed devices**

  If this option is selected, the remote installation task is created for a group of devices.

- **Select devices for installation**

  The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.




Specifying the list of devices on which the application will be installed

# Step 6. Specifying the remote installation task settings

On the **Remote installation task settings** page, specify the settings for remote installation of the application.

In the **Force installation package download** settings group, specify how files that are required for the application installation are distributed to client devices:

- **Using Network Agent**

  If this option is enabled, installation packages are delivered to client devices by Network Agent installed on those client devices.

  If this option is disabled, installation packages are delivered using the operating system tools of client devices.

  We recommend that you enable this option if the task has been assigned to devices with Network Agents installed.

  By default, the option is enabled.

- **Using operating system resources through distribution points**

  If the check box is selected, the installation packages are delivered to client devices using the operating system's mechanisms through distribution point. You can select this option if there is at least one distribution point on the network.

  If the **Using Network Agent** option is enabled, the files are delivered using operating system tools only if Network Agent tools are unavailable.

  By default, this option is enabled for remote installation tasks that have been created on a virtual Administration Server.

The only way to install an application for Windows (including Network Agent for Windows) on a device that does not have Network Agent installed is by using a Windows-based distribution point. Therefore, when you install a Windows application:

- Select this option.
- Ensure that a distribution point is assigned for the target client devices.
- Ensure the distribution point is Windows-based.

- **Using operating system resources through Administration Server**

  If this option is enabled, files are transmitted to client devices by using operating system tools of client devices through the Administration Server. You can enable this option if no Network Agent is installed on the client device, but the client device is in the same network as the Administration Server.

  By default, the option is enabled.

Define the additional setting:

- **Do not re-install application if it is already installed**

  If this option is enabled, the selected application will not be re-installed if it has already been installed on this client device.

  If this option is disabled, the application will be installed anyway.

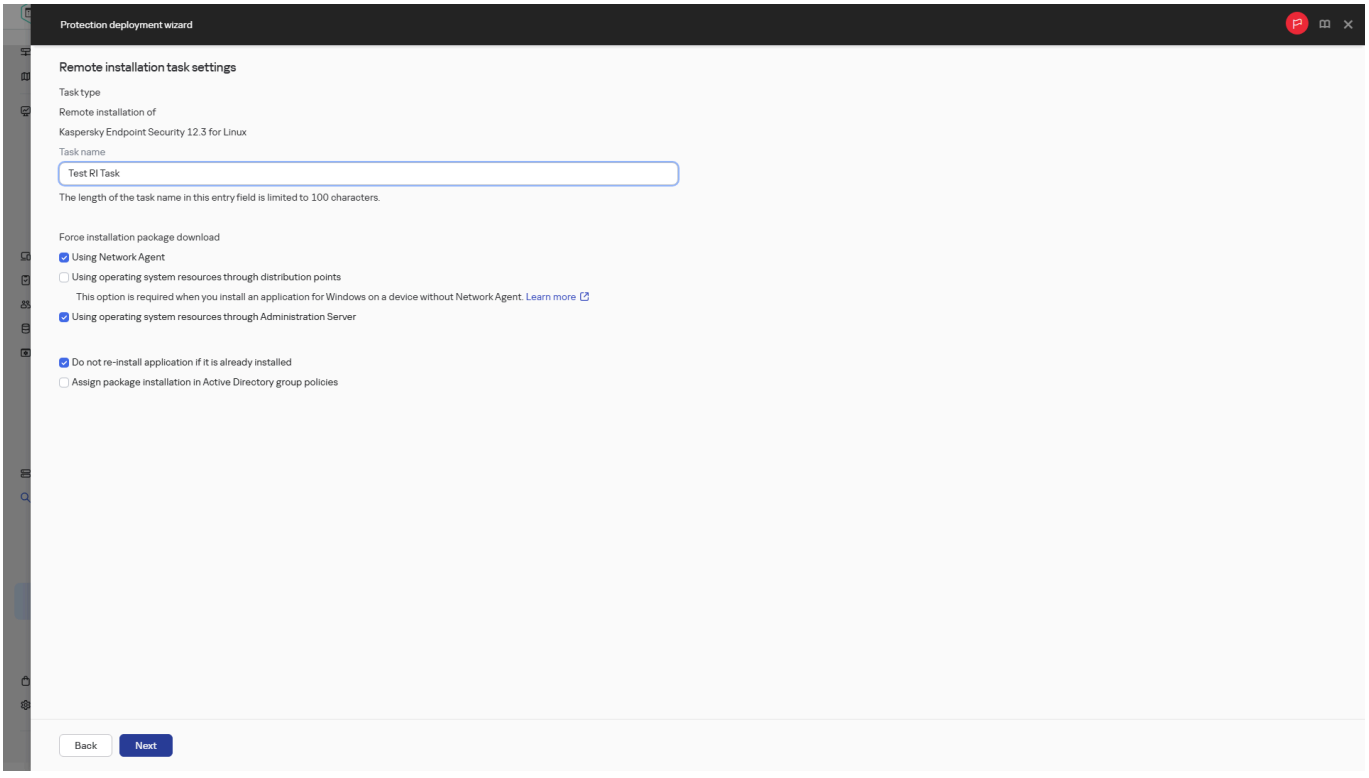
  By default, the option is enabled.

- **Assign package installation in Active Directory group policies**

  If this option is enabled, an installation package is installed by using the Active Directory group policies.

  This option is available if the Network Agent installation package is selected.

  By default, this option is disabled.




Specifying the remote installation task settings

# Step 7. Restart management

Specify the action to be performed if the operating system must be restarted when you install the application:

- **Do not restart the device**

  Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

  Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

  The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

  By default, this option is selected.

  - **Repeat prompt every (min)**

    If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

    By default, the option is enabled. The default interval is 5 minutes. Available values are between 1 and 1440 minutes.

    If this option is disabled, the prompt is displayed only once.

  - **Restart after (min)**

    After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

    By default, the option is enabled. The default delay is 30 minutes. Available values are between 1 and 1440 minutes.

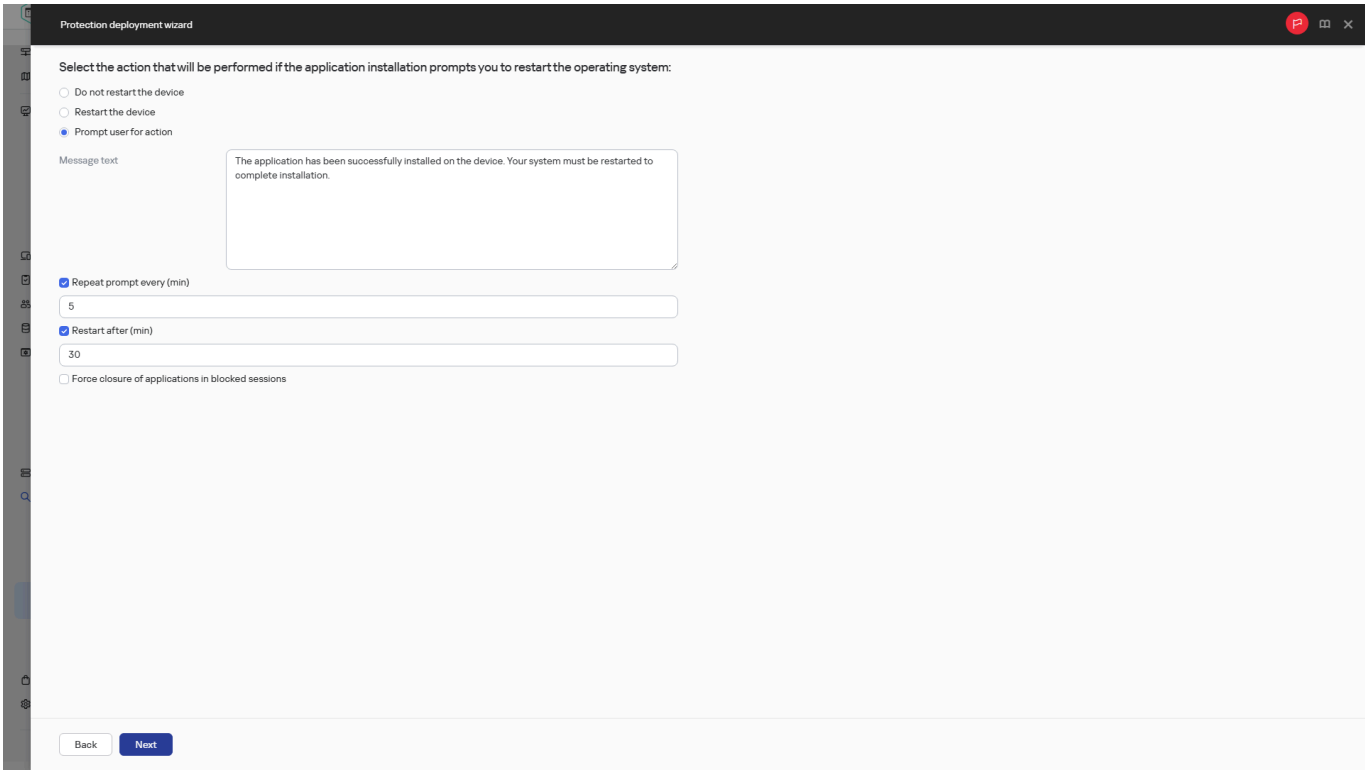
- **Force closure of applications in blocked sessions**

  Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

  If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

  If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.




Selecting the operating system restart option

# Step 8. Removing incompatible applications before installation

This step is only present if the application that you deploy is known to be incompatible with some other applications.

Select the option if you want Kaspersky Security Center Linux to automatically remove applications that are incompatible with the application you deploy.

The list of incompatible applications is also displayed.

If you do not select this option, the application will only be installed on devices that have no incompatible applications.

# Step 9. Moving devices to Managed devices

Specify whether devices must be moved to an administration group after Network Agent installation.

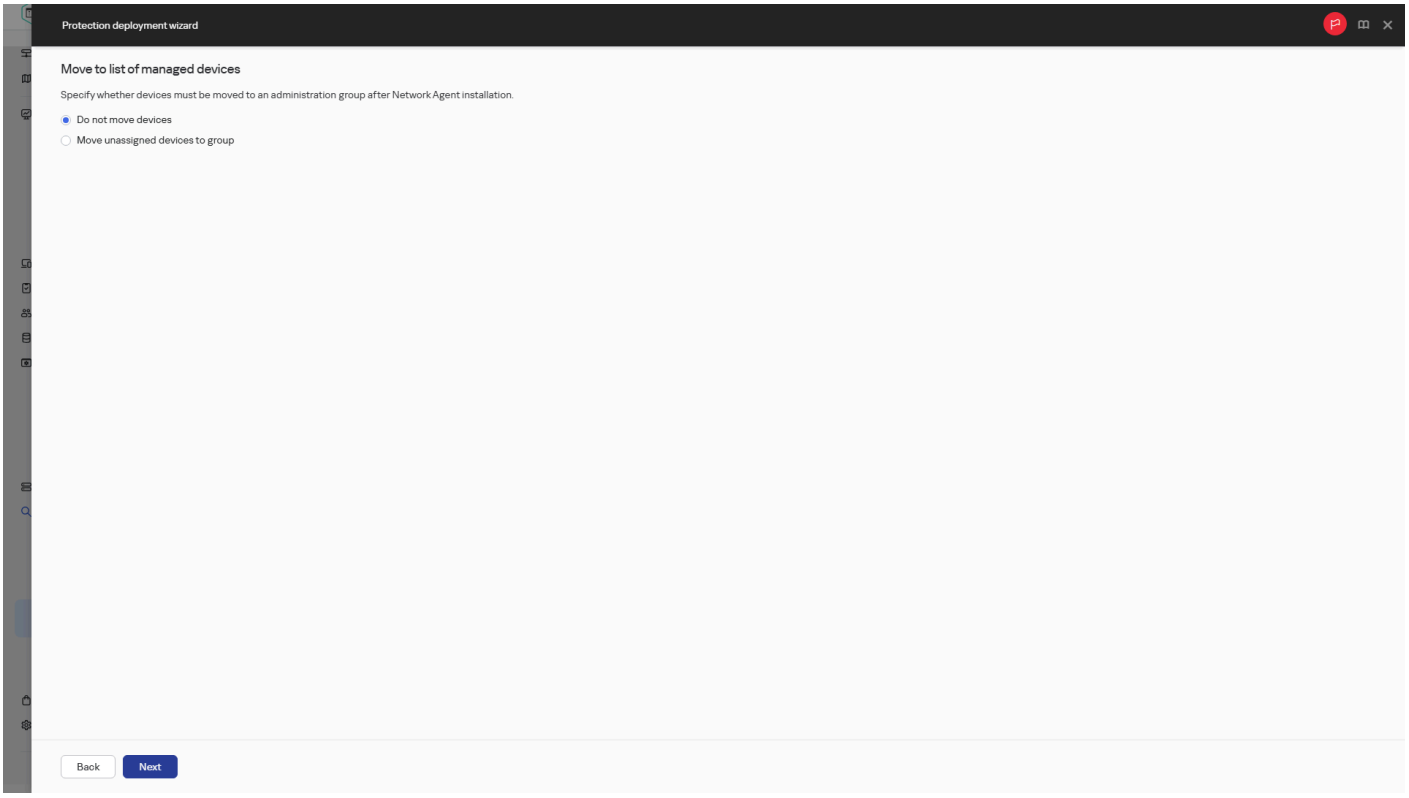
- **Do not move devices**

  The devices remain in the groups in which they are currently located. The devices that have not been placed in any group remain unassigned.

- **Move unassigned devices to group**

  The devices are moved to the administration group that you select.

The **Do not move devices** option is selected by default. For security reasons, you might want to move the devices manually.




Selecting an option to move devices to an administration group

# Step 10. Selecting accounts to access devices

If necessary, add the accounts that will be used to start the remote installation task:

- **No account required (Network Agent installed)**

  If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running.

  If Network Agent has not been installed on client devices, this option is not available.

- **Account required (Network Agent is not used)**

  Select this option if Network Agent is not installed on the devices for which you assign the remote installation task. In this case, you can specify a user account or an SSH certificate to install the application.

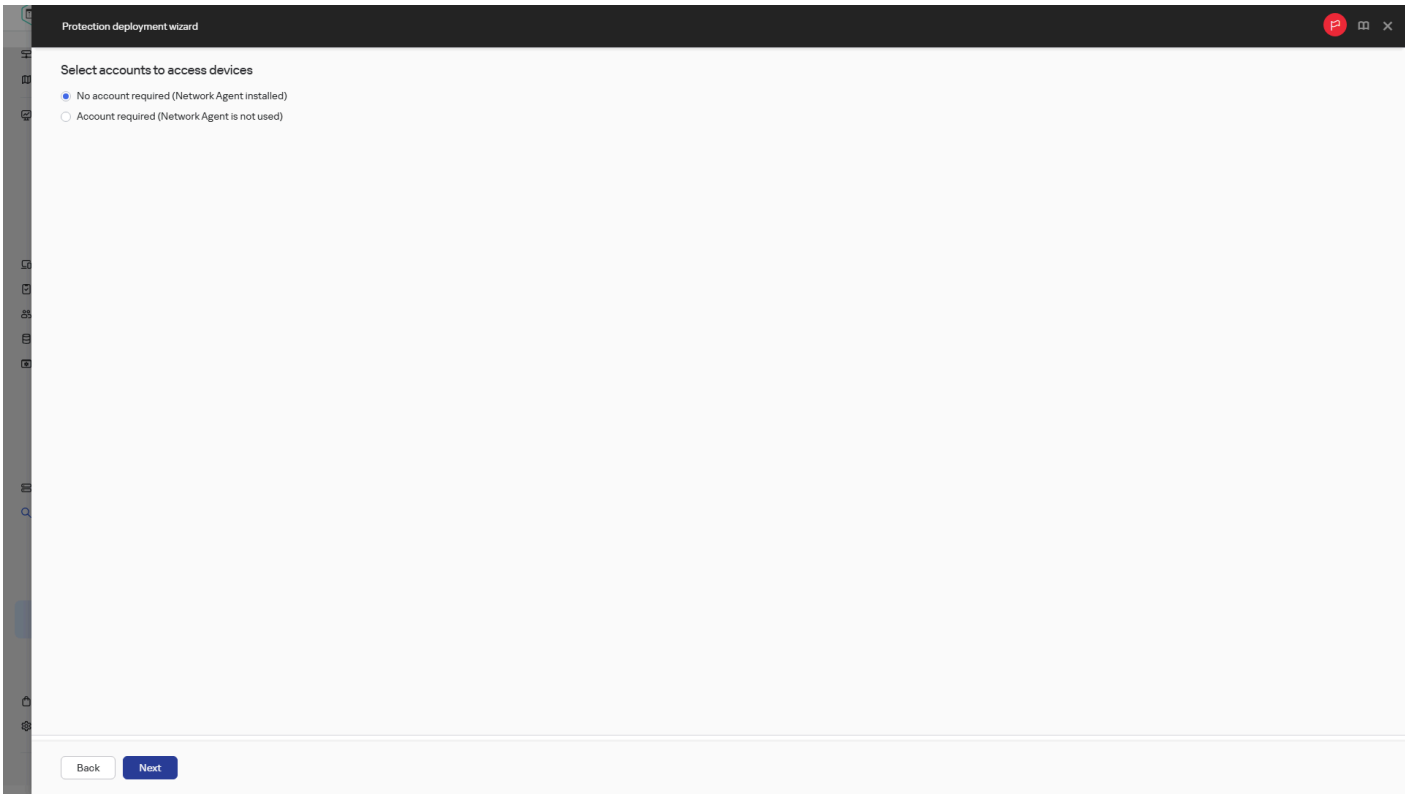
  - **Local or domain account**. If this option is selected, specify the user account under which the application installer will be run. Click the **Add** button, select **Local or domain account**, and then specify the user account credentials.

    You can specify multiple user accounts if, for example, none of them have all the required rights on all devices for which you assign the task. In this case, all added accounts are used for running the task, in consecutive order, top-down.

  - **SSH certificate**. If you want to install an application on a Linux-based client device, you can specify an SSH certificate instead of a user account. Click the **Add** button, select **SSH certificate**, and then specify the private and public keys of the certificate.

To generate a private key, you can use the ssh-keygen utility. Note that Kaspersky Security Center Linux supports the PEM format of private keys, but the ssh-keygen utility generates SSH keys in the OPENSSH format by default. The OPENSSH format is not supported by Kaspersky Security Center Linux. To create a private key in the supported PEM format, add the -m PEM option in the ssh-keygen command. For example:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
```




Selecting accounts to access devices

# Step 11. Starting installation

This page is the final step of the wizard. At this step, the **Remote installation task** has been successfully created and configured.

By default, the **Run the task after the wizard finishes** option is not selected. If you select this option, the **Remote installation task** will start immediately after you complete the wizard. If you do not select this option, the **Remote installation task** will not start. You can later start this task manually.

Click **OK** to complete the final step of the Protection deployment wizard.

# Upgrading Kaspersky Security Center Linux

You can install version 17 of Administration Server on a device that has an earlier version of Administration Server installed (starting from version 13). When upgrading to version 17, all data and settings from the previous version of Administration Server are preserved.

## Prerequisites

- Create a backup copy of the Administration Server data before starting the upgrade.
- When upgrading Administration Server from version 16 or earlier to version 16.1 or later, two-factor authentication is enabled. For more information, refer to About two-factor authentication for an account.

  To ensure that users can sign in to Web Console with their existing accounts by using configured two-factor authentication secret keys, and that OpenAPI automation scripts continue to work after the upgrade, you must perform the following steps:

  - Enable two-factor authentication for all users
  - Administrators must configure two-factor authentication for their own accounts
  - Excluding accounts from two-factor authentication

    If needed, add integration accounts used to run scripts through OpenAPI to the exclusion list.
- Ensure that you use the versions of the operating system and DBMS that are supported by version 17 of Administration Server. If necessary, you can move Administration Server to another device with later versions of the operating system and DBMS.
- When upgrading Administration Server from version 15.4 or earlier to version 16 or later, on the DBMS server, create a database for IAM. The database name must be different from the database that you installed to work with Kaspersky Security Center Linux.

  - For PostgreSQL, run the following command:

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```
  - For MariaDB, run the following command:

    ```
    sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
    ```
- When upgrading Administration Server from version 15.4 or earlier to version 16 or later, prepare the answer file with new parameters for IAM. For the list of the required parameters, refer to the article Installing Kaspersky Security Center Linux in silent mode. Add the `KLAUTOANSWERS` environment variable. Set the value of the variable to the path to the answers file.
- Make available the port used by the kliam process for the OpenID Connect protocol authentication. The default value is 4444. Refer to the `trusted` parameter description in the following article: Kaspersky Security Center Web Console installation parameters.

## Stages

### 1 Upgrading of Administration Server

You can upgrade a version of Administration Server by using one of the following methods:

- By using the Kaspersky Security Center Linux installation file
- By creating the Administration Server data backup, installing a new Administration Server version, and restoring the Administration Server data from the backup

> During the upgrade, concurrent use of the DBMS by Administration Server and another application is strictly forbidden.

If your network includes several Administration Servers, you have to upgrade every Server manually. Kaspersky Security Center Linux does not support centralized upgrade.

### 2 Running the postinstall.pl script (optional step)

If the answer file does not include IAM parameters or the answer file is not found, a message is shown in the terminal during upgrade that asks you to run the postinstall.pl script.

At this stage of the scenario, do the following:

1. In the Administration Server operating system, create an unprivileged user account 'ksciam' that must be a member of the 'kladmins' group:

   ```
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

2. Under an account with root privileges, run the /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl script to configure the Administration Server after upgrade. When prompted, enter the following settings:

   1. Enter the IAM Server FQDN. You must use the Administration Server DNS name that was specified when installing Kaspersky Security Center Linux.
   2. Enter the account name to start the IAM service. The account must be a member of the entered security group. By default, the ksciam account is used.
   3. Select the DBMS that you installed to work with the IAM service:
      - If you installed MySQL or MariaDB, enter 1.
      - If you installed PostgreSQL or Postgres Pro, enter 2.
   4. Enter the IAM DBMS address to be used by the IAM service.

5. Enter the IAM DBMS port number. This port is used to communicate with the IAM service. By default, the following ports are used:

   - Port 3306 for MySQL or MariaDB.
   - Port 5432 for PostgreSQL or Postgres Pro.

6. Enter the IAM database name to be used by the IAM service. The name of the database used by IAM service should be different from database used by the Administration Server.

3. Upgrading Kaspersky Security Center Web Console
4. **(Optional) Upgrading Network Agent on devices to a new version.**
5. **Ensuring that the two-factor authentication allowlist contains only the user accounts that must have access to Administration Server.**

   Review the two-factor authentication allowlist and remove any other accounts from it.

Note that if you upgrade the Administration Server to the version 17, you will not be able to create new installation packages of Network Agent version 15 or earlier. However, previously created installation packages will be available.

When you upgrade Kaspersky Security Center Linux from a previous version, all the installed plug-ins of supported Kaspersky applications are kept. Administration Server plug-in and Network Agent plug-in are upgraded automatically.

# Upgrading Kaspersky Security Center Linux from version 16 or later

This section describes the following options for upgrading Kaspersky Security Center Linux from version 16 or later to the latest version:

- Upgrading by using the installation file
- Upgrading through backup
- Upgrading on the Kaspersky Security Center Linux failover cluster nodes

## Upgrading Kaspersky Security Center Linux from version 16 or later by using the installation file

To upgrade Administration Server from version 16 or later to the latest version, you can install a new version over an earlier one by using the Kaspersky Security Center Linux installation file.

*To upgrade Kaspersky Security Center Linux from version 16 or later to the latest version by using the installation file:*

1. Download the Kaspersky Security Center Linux installation file with a full package for version 17 from the Kaspersky website:
   - For devices running an RPM-based operating system—`ksc64-<version number>.x86_64.rpm`
   - For devices running a Debian-based operating system—`ksc64_<version number>_amd64.deb`
2. Start upgrading Kaspersky Security Center Linux. Run one of the following commands in the command-line terminal:
   - For devices running an RPM-based operating system:

     ```
     sudo yum install ./ksc64-<version number>.x86_64.rpm
     ```

   - For devices running a Debian-based operating system:

     ```
     sudo apt-get install ./ksc64_<version number>_amd64.deb
     ```

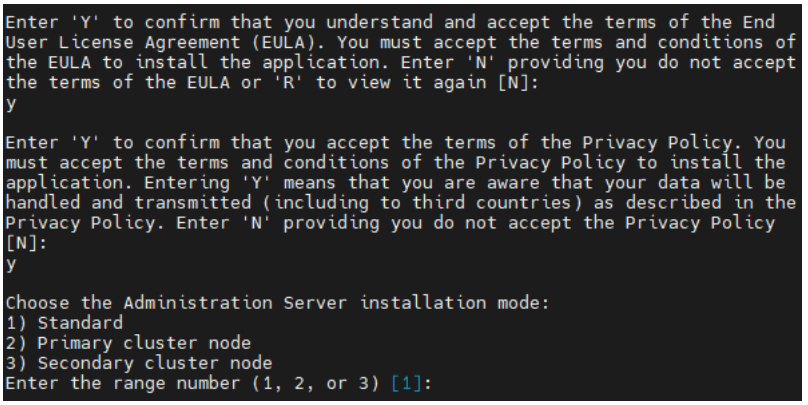
   After the command has been successfully executed, the `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` script is created. The message about that is displayed in the terminal.
3. Run the `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` script to configure the upgraded Administration Server:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

4. Read the License Agreement and Privacy Policy, which appear in the command-line terminal. If you agree with all of the terms of the License Agreement and Privacy Policy:
   a. Enter `Y` to confirm that you have fully read, understood, and accept the terms and conditions of the EULA.
   b. Enter `Y` again to confirm that you have fully read, understood, and accept the Privacy Policy that describes the handling of data.

   Installation of the application on your device will continue after you have entered `Y` twice.
5. Enter `1` to select the standard Administration Server installation mode.

The picture below shows the last two steps.




Accepting the terms of the EULA and the Privacy Policy, and selecting the standard Administration Server installation mode in the command-line terminal

Next, the script configures and finishes upgrading the Administration Server. During the upgrade, you cannot change the Administration Server settings adjusted before the upgrade.

6. Upgrade Kaspersky Security Center Web Console to a new version.

7. For devices on which the earlier version of Network Agent was installed, create and run the task for remote installation of the new Network Agent version.

   We recommend that you upgrade Network Agent for Linux to the same version as Kaspersky Security Center Linux.

   After completion of the remote installation task, the Network Agent version is upgraded.

   Run the following commands on Linux-based assets to remove dependencies that are no longer needed:

   - For Debian-based assets, run either of the following commands:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - For RPM-based assets, run either of the following commands:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

# Upgrading Kaspersky Security Center Linux from version 16 or later through backup

To upgrade Administration Server from version 16 or later to the latest version, you can create a backup of the Administration Server data and restore this data after installing Kaspersky Security Center Linux of a new version. If problems occur during installation, you can restore the previous version of Administration Server by using the backup of the Administration Server data created before the upgrade.

*To upgrade Kaspersky Security Center Linux from version 16 or later to the latest version through backup:*

1. Before the upgrade, back up the Administration Server data with an older version of the application.
2. Uninstall the older version of Kaspersky Security Center Linux.
3. Install Kaspersky Security Center Linux version 17 on the device where Administration Server was previously installed.

   If the database schema in the backup copy differs from the one currently used by Administration Server or IAM, the data will be restored to the current schema.

   If public schema is used in the backup copy, the following conditions must be met:

   - Public database schema exists in the database.
   - You can modify the public database schema from the DBMS account used by Administration Server or IAM to access the database.

   Otherwise, the data restore ends with an error.
4. Restore the Administration Server data from the backup created before the upgrade.
5. Install Kaspersky Security Center Web Console.

   If Kaspersky Security Center Web Console was installed earlier, reinstall it with the same response file.

   Log in to Kaspersky Security Center Web Console under the administrator's internal user account.

   The data initialization process usually takes up to 15 minutes after restoring Administration Server data, but the time depends on the hardware performance and the size of the Administration Server data. During this time, Kaspersky Security Center Web Console may fail to connect and display errors.
6. For devices on which the earlier version of Network Agent was installed, create and run the task for remote installation of the new Network Agent version.

   > We recommend that you upgrade Network Agent for Linux to the same version as Kaspersky Security Center Linux.

   After completion of the remote installation task, the Network Agent version is upgraded.

Run the following commands on Linux-based assets to remove dependencies that are no longer needed:

- For Debian-based assets, run either of the following commands:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- For RPM-based assets, run either of the following commands:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

# Upgrading Kaspersky Security Center Linux from version 16 or later on the Kaspersky Security Center Linux failover cluster nodes

You can install the latest Administration Server version on every Kaspersky Security Center Linux failover cluster node where Administration Server version 16 or later is installed. When upgrading to the latest version, all data and settings from the previous version of Administration Server are preserved.

If you previously installed Kaspersky Security Center Linux on devices locally, you can also upgrade Kaspersky Security Center Linux on these devices by using the installation file or through backup.

Upgrading Kaspersky Security Center Linux to version 17 on failover cluster nodes using an installation file is not supported. To upgrade from a previous version to version 17, create a backup copy of the Administration Server data, install the new version of the Kaspersky Security Center Linux failover cluster, then restore the Administration Server data from the backup copy. This limitation also applies to a geographically distributed cluster.

*To upgrade Kaspersky Security Center Linux from version 16 or later on the Kaspersky Security Center Linux failover cluster nodes:*

1. Download the Kaspersky Security Center Linux installation file with a full package for version 17 from the Kaspersky website:
   - For devices running an RPM-based operating system—`ksc64-<version number>-<build number>.x86_64.rpm`
   - For devices running a Debian-based operating system—`ksc64_<version number>-<build number>_amd64.deb`
2. Stop the cluster.

3. On the active node of the cluster, run the following command in the command-line terminal to run upgrading:

   - For devices running an RPM-based operating system:

     ```
     sudo yum install ./ksc64-<version number>-<build number>.x86_64.rpm
     ```

   - For devices running a Debian-based operating system:

     ```
     sudo apt-get install ./ksc64_<version number>-<build number>_amd64.deb
     ```

   After the command has been successfully executed, the `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` script is created. The message about that is displayed in the terminal.

   If any errors occur, see the solution described in the Knowledge Base.

4. Run the `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` script to configure the upgraded Administration Server:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Read the License Agreement and Privacy Policy, which appear in the command-line terminal. If you agree with all of the terms of the License Agreement and Privacy Policy:

   a. Enter `Y` to confirm that you have fully read, understood, and accept the terms and conditions of the EULA.

   b. Enter `Y` again to confirm that you have fully read, understood, and accept the Privacy Policy that describes the handling of data.

   Installation of the application on your device will continue after you have entered `Y` twice.

6. Select the node on which you are upgrading by entering `2`.

   The picture below shows the last two steps.

   ```
   Enter 'Y' to confirm that you understand and accept the terms of the End
   User License Agreement (EULA). You must accept the terms and conditions of
   the EULA to install the application. Enter 'N' providing you do not accept
   the terms of the EULA or 'R' to view it again [N]:
   y

   Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
   must accept the terms and conditions of the Privacy Policy to install the
   application. Entering 'Y' means that you are aware that your data will be
   handled and transmitted (including to third countries) as described in the
   Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
   [N]:
   y

   Choose the Administration Server installation mode:
   1) Standard
   2) Primary cluster node
   3) Secondary cluster node
   Enter the range number (1, 2, or 3) [1]:
   ```

   Accepting the terms of the EULA and the Privacy Policy, and selecting the installation mode in the command-line terminal

   Next, the script configures and finishes upgrading the Administration Server. During the upgrade, you cannot change the Administration Server settings adjusted before the upgrade.

7. Perform steps 3–5 on the passive node.

   At step 6, enter `3` to select the node.

8. Start the cluster.

   You can start the cluster on any node. If you start the cluster on the passive node, it becomes the active node.

9. For devices on which the earlier version of Network Agent is installed, create and run the task for remote installation of the new version of Network Agent.

   We recommend that you upgrade Network Agent for Linux to the same version as Kaspersky Security Center Linux.

   After completion of the remote installation task, the Network Agent version is upgraded.

   Run the following commands on Linux-based assets to remove dependencies that are no longer needed:

   - For Debian-based assets, run either of the following commands:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - For RPM-based assets, run either of the following commands:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

   As a result, you installed the Administration Server of the latest version on the Kaspersky Security Center Linux failover cluster nodes.

# Upgrading Kaspersky Security Center Linux from version 15.4 or earlier

This section describes the following options for upgrading Kaspersky Security Center Linux from version 15.4 or earlier to version 16 or later:

- Upgrading by using the installation file
- Upgrading through backup
- Upgrading on the Kaspersky Security Center Linux failover cluster nodes

Each upgrade option Kaspersky Security Center Linux from version 15.4 or earlier to version 16 or later includes steps to create and configure an IAM database on a DBMS server, create an unprivileged 'ksciam' account to run the IAM service, and add this account to the 'kladmins' security group.

# Upgrading Kaspersky Security Center Linux from version 15.4 or earlier by using the installation file

To upgrade Administration Server from version 13—15.4 to version 16 or later, you can install a new version over an earlier one by using the Kaspersky Security Center Linux installation file.

**Before you start, check the requirements to a custom certificate.**

If you are using custom certificate instead of the self-signed one, before upgrading Kaspersky Security Center Linux to the later version, you have to make sure that the certificate includes the Subject Alternative Name (SAN). If not, is important to replace the certificate before upgrading Kaspersky Security Center Linux. Otherwise, you will not be able to sign in to Web Console after upgrade.

*To make sure that the certificate includes SAN:*

1. On the device with Administration Server installed, execute the command:

   - For a Linux-based device:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - For a Windows-based device:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Make sure that the Subject Alternative Name (SAN) is present in the command output and contains the address of the Administration Server device.

3. If the Subject Alternative Name is missing, use the klsetsrvcert utility to replace your user certificate with a certificate that meets the requirements.

*To upgrade Kaspersky Security Center Linux from version 15.4 or earlier to the latest version by using the installation file:*

1. Download the Kaspersky Security Center Linux installation file with a full package for version 17 from the Kaspersky website:

   - For devices running an RPM-based operating system—`ksc64-<version number>.x86_64.rpm`
   - For devices running a Debian-based operating system—`ksc64_<version number>_amd64.deb`

2. On the DBMS server, create a database for IAM. The database IAM name must be different from the database that you installed to work with Kaspersky Security Center Linux.

   - For PostgreSQL, run the following command:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - For MariaDB, run the following command:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. Create an unprivileged account 'ksciam', add it to the 'kladmins' security group, and then set the 'kladmins' group as the primary group for the 'ksciam' account. To do this, sequentially run the following commands:

```
sudo adduser ksciam
sudo gpasswd -a ksciam kladmins
sudo usermod -g kladmins ksciam
```

4. Start upgrading Kaspersky Security Center Linux. Run one of the following commands in the command-line terminal:

   - For devices running an RPM-based operating system:

     ```
     sudo yum install ./ksc64-<version number>.x86_64.rpm
     ```

   - For devices running a Debian-based operating system:

     ```
     sudo apt-get install ./ksc64_<version number>_amd64.deb
     ```

   After the command has been successfully executed, the `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` script is created. The message about that is displayed in the terminal.

5. Run the `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` script to configure the upgraded Administration Server:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

6. Read the License Agreement and Privacy Policy, which appear in the command-line terminal. If you agree with all of the terms of the License Agreement and Privacy Policy:

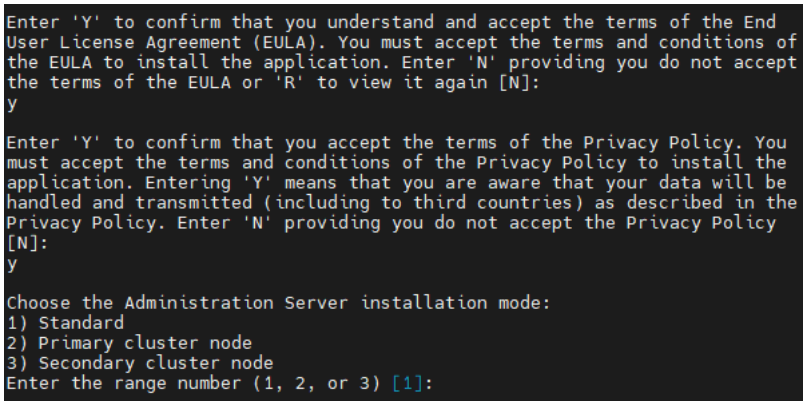
   a. Enter `Y` to confirm that you have fully read, understood, and accept the terms and conditions of the EULA.

   b. Enter `Y` again to confirm that you have fully read, understood, and accept the Privacy Policy that describes the handling of data.

   Installation of the application on your device will continue after you have entered `Y` twice.

7. Enter `1` to select the standard Administration Server installation mode.

   The picture below shows the last two steps.




Accepting the terms of the EULA and the Privacy Policy, and selecting the standard Administration Server installation mode in the command-line terminal

8. Next, the script configures and finishes upgrading the Administration Server. During the upgrade, you cannot change the Administration Server settings adjusted before the upgrade. When prompted, enter the following settings:

   a. Enter the IAM Server FQDN.

      You must use the Administration Server DNS name that was specified when installing Kaspersky Security Center Linux.

   b. Enter the account name to start the IAM service. The account must be a member of the entered security group. By default, the ksciam account is used.

   c. Select the DBMS that you installed to work with the IAM service:

      - If you installed MySQL or MariaDB, enter `1`.
      - If you installed PostgreSQL or Postgres Pro, enter `2`.

   d. Enter the IAM DBMS address to be used by the IAM service.

   e. Enter the IAM DBMS port number. This port is used to communicate with the IAM service. By default, the following ports are used:

      - Port 3306 for MySQL or MariaDB.
      - Port 5432 for PostgreSQL or Postgres Pro.

   f. Enter the IAM database name to be used by the IAM service. The name of the database used by IAM service should be different from database used by the Administration Server.

   g. Enter the DBMS login and password to be used by the IAM service.

   h. If you installed PostgreSQL or Postgres Pro, you can specify the database schema to be used by IAM. To do it, specify the schema name.

      If you do not want to use a custom schema, press `ENTER`, and a default schema will be used.

      > The schema name is case-sensitive: you have to use only lowercase letters.
      > Do not specify the reserved iam schema names: `client, iam, ksc, locker, pat, scope, voltron`.

9. Upgrade Kaspersky Security Center Web Console to a new version.

10. For devices on which the earlier version of Network Agent was installed, create and run the task for remote installation of the new Network Agent version.

    > We recommend that you upgrade Network Agent for Linux to the same version as Kaspersky Security Center Linux.

    After completion of the remote installation task, the Network Agent version is upgraded.

Run the following commands on Linux-based assets to remove dependencies that are no longer needed:

- For Debian-based assets, run either of the following commands:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- For RPM-based assets, run either of the following commands:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

# Upgrading Kaspersky Security Center Linux from version 15.4 or earlier through backup

To upgrade Administration Server from version 14.2–15.4 to version 16 or later, you can create a backup of the Administration Server data and restore it after installing a new version of Kaspersky Security Center Linux. If problems occur during installation, you can restore the previous version of Administration Server by using the backup of the Administration Server data created before the upgrade.

Prerequisites

1. **Check the requirements to a custom certificate.**

   If you are using custom certificate instead of the self-signed one, before upgrading Kaspersky Security Center Linux to the later version, you have to make sure that the certificate includes the Subject Alternative Name (SAN). If not, is important to replace the certificate before upgrading Kaspersky Security Center Linux. Otherwise, you will not be able to sign in to Web Console after upgrade.

   *To make sure that the certificate includes SAN:*

   1. On the device with Administration Server installed, execute the command:

      - For a Linux-based device:

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - For a Windows-based device:

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

2. Make sure that the Subject Alternative Name (SAN) is present in the command output and contains the address of the Administration Server device.

3. If the Subject Alternative Name is missing, use the klsetsrvcert utility to replace your user certificate with a certificate that meets the requirements.

2. Back up the Administration Server data with an older version of the application.

The upgrade procedure

*To upgrade Kaspersky Security Center Linux from version 15.4 or earlier to the latest version through backup:*

1. Uninstall the older version of Kaspersky Security Center Linux.

2. On the DBMS server, create a database for IAM. The database IAM name must be different from the database that you installed to work with Kaspersky Security Center Linux.

   - For PostgreSQL, run the following command:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - For MariaDB, run the following command:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. Create an unprivileged account 'ksciam', add it to the 'kladmins' security group, and then set the 'kladmins' group as the primary group for the 'ksciam' account. To do this, sequentially run the following commands:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

4. Install Kaspersky Security Center Linux version 17 on the device where Administration Server was previously installed.

   If the database schema in the backup copy differs from the one currently used by Administration Server or IAM, the data will be restored to the current schema.

   If public schema is used in the backup copy, the following conditions must be met:

   - Public database schema exists in the database.

   - You can modify the public database schema from the DBMS account used by Administration Server or IAM to access the database.

   Otherwise, the data restore ends with an error.

5. Restore the Administration Server data from the backup created before the upgrade.

6. Configure certificate verification by Administration Server and IAM Server.

7. Install Kaspersky Security Center Web Console.

If Kaspersky Security Center Web Console was installed earlier, reinstall it with the same response file.

Log in to Kaspersky Security Center Web Console under the administrator's internal user account.

The data initialization process usually takes up to 15 minutes after restoring Administration Server data, but the time depends on the hardware performance and the size of the Administration Server data. During this time, Kaspersky Security Center Web Console may fail to connect and display errors.

8. For devices on which the earlier version of Network Agent was installed, create and run the task for remote installation of the new Network Agent version.

   We recommend that you upgrade Network Agent for Linux to the same version as Kaspersky Security Center Linux.

   After completion of the remote installation task, the Network Agent version is upgraded.

   Run the following commands on Linux-based assets to remove dependencies that are no longer needed:

   - For Debian-based assets, run either of the following commands:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - For RPM-based assets, run either of the following commands:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

# Upgrading Kaspersky Security Center Linux from version 15.4 or earlier on the Kaspersky Security Center Linux failover cluster nodes

You can install Administration Server version 16 or later on every Kaspersky Security Center Linux failover cluster node where the Administration Server version 14—15.4 is installed. When upgrading, all data and settings from the previous version of Administration Server are preserved.

**Before you start, check the requirements to a custom certificate.**

If you are using custom certificate instead of the self-signed one, before upgrading Kaspersky Security Center Linux to the later version, you have to make sure that the certificate includes the Subject Alternative Name (SAN). If not, is important to replace the certificate before upgrading Kaspersky Security Center Linux. Otherwise, you will not be able to sign in to Web Console after upgrade.

*To make sure that the certificate includes SAN:*

1. On the device with Administration Server installed, execute the command:

   - For a Linux-based device:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - For a Windows-based device:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Make sure that the Subject Alternative Name (SAN) is present in the command output and contains the address of the Administration Server device.

3. If the Subject Alternative Name is missing, use the klsetsrvcert utility to replace your user certificate with a certificate that meets the requirements.

If you previously installed Kaspersky Security Center Linux on devices locally, you can also upgrade Kaspersky Security Center Linux on these devices by using the installation file or through backup.

*To upgrade Kaspersky Security Center Linux from version 15.4 or earlier on the Kaspersky Security Center Linux failover cluster nodes:*

1. Download the Kaspersky Security Center Linux installation file with a full package for version 17 from the Kaspersky website:

   - For devices running an RPM-based operating system—`ksc64-<version number>-<build number>.x86_64.rpm`

   - For devices running a Debian-based operating system—`ksc64_<version number>-<build number>_amd64.deb`

2. Stop the cluster.

3. On the DBMS server, create a database for IAM. The database IAM name must be different from the database that you installed to work with Kaspersky Security Center Linux.

   - For PostgreSQL, run the following command:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - For MariaDB, run the following command:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

4. Create an unprivileged account 'ksciam', add it to the 'kladmins' security group, and then set the 'kladmins' group as the primary group for the 'ksciam' account. To do this, sequentially run the following commands:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

5. On the active node of the cluster, run one the following commands on the command line to start the upgrade:

   - For devices running an RPM-based operating system:

     ```
     sudo yum install ./ksc64-<version number>-<build number>.x86_64.rpm
     ```

   - For devices running a Debian-based operating system:

     ```
     sudo apt-get install ./ksc64_<version number>-<build number>_amd64.deb
     ```

   After the command has been successfully executed, the `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` script is created. The message about that is displayed in the terminal.

6. Run the `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` script to configure the upgraded Administration Server:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

7. Read the License Agreement and Privacy Policy, which appear in the command-line terminal. If you agree with all of the terms of the License Agreement and Privacy Policy:

   a. Enter `Y` to confirm that you have fully read, understood, and accept the terms and conditions of the EULA.

   b. Enter `Y` again to confirm that you have fully read, understood, and accept the Privacy Policy that describes the handling of data.

   Installation of the application on your device will continue after you have entered `Y` twice.

8. Select the node on which you are upgrading by entering `2`.

   The picture below shows the last two steps.

   ```
   Enter 'Y' to confirm that you understand and accept the terms of the End
   User License Agreement (EULA). You must accept the terms and conditions of
   the EULA to install the application. Enter 'N' providing you do not accept
   the terms of the EULA or 'R' to view it again [N]:
   y

   Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
   must accept the terms and conditions of the Privacy Policy to install the
   application. Entering 'Y' means that you are aware that your data will be
   handled and transmitted (including to third countries) as described in the
   Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
   [N]:
   y

   Choose the Administration Server installation mode:
   1) Standard
   2) Primary cluster node
   3) Secondary cluster node
   Enter the range number (1, 2, or 3) [1]:
   ```

   Accepting the terms of the EULA and the Privacy Policy, and selecting the installation mode in the command-line terminal

9. Next, the script configures and finishes upgrading the Administration Server. During the upgrade, you cannot change the Administration Server settings adjusted before the upgrade. When prompted, enter the following settings:

   a. Enter the IAM Server FQDN.

   You must use the Administration Server DNS name that was specified when installing Kaspersky Security Center Linux.

b. Enter the account name to start the IAM service. The account must be a member of the entered security group. By default, the ksciam account is used.

c. Select the DBMS that you installed to work with the IAM service:

- If you installed MySQL or MariaDB, enter `1`.
- If you installed PostgreSQL or Postgres Pro, enter `2`.

d. Enter the IAM DBMS address to be used by the IAM service.

e. Enter the IAM DBMS port number. This port is used to communicate with the IAM service. By default, the following ports are used:

- Port 3306 for MySQL or MariaDB.
- Port 5432 for PostgreSQL or Postgres Pro.

f. Enter the IAM database name to be used by the IAM service. The name of the database used by IAM service should be different from database used by the Administration Server.

g. Enter the DBMS login and password to be used by the IAM service.

10. Perform the step 5 on the passive node.

    At step 6, enter `3` to select the node.

11. Start the cluster.

    You can start the cluster on any node. If you start the cluster on the passive node, it becomes the active node.

12. For devices on which the earlier version of Network Agent is installed, create and run the task for remote installation of the new version of Network Agent.

    We recommend that you upgrade Network Agent for Linux to the same version as Kaspersky Security Center Linux.

    After completion of the remote installation task, the Network Agent version is upgraded.

    Run the following commands on Linux-based assets to remove dependencies that are no longer needed:

    - For Debian-based assets, run either of the following commands:

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

- For RPM-based assets, run either of the following commands:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

As a result, you installed the Administration Server of the latest version on the Kaspersky Security Center Linux failover cluster nodes.

# Upgrading Kaspersky Security Center Web Console

This article describes how to upgrade Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) on devices running the Linux operating system.

If you need to upgrade Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode, follow the instructions specific for Astra Linux.

Use one of the following installation files that corresponds to the Linux distribution installed on your device:

- For Debian-based operating systems: ksc-web-console-<build_number>.x86_64.deb
- For RPM-based operating systems: ksc-web-console-<build_number>.x86_64.rpm

You receive the installation file by downloading it from the Kaspersky website.

*To upgrade Kaspersky Security Center Web Console:*

1. Make sure that the device on which you want to upgrade Kaspersky Security Center Web Console is running one of the supported Linux distributions.
2. Read and accept the End User License Agreement (EULA). If the Kaspersky Security Center Linux distribution kit does not include a TXT file with the text of EULA, you can download the file from the Kaspersky website. If you do not accept the terms of the License Agreement, do not upgrade Kaspersky Security Center Web Console by using the installation file.
3. Use the same response file that you prepared before installing Kaspersky Security Center Web Console. The response file name is ksc-web-console-setup.json. The file location is /etc/ksc-web-console-setup.json.

   If when installing Kaspersky Security Center Web Console you specified the values for the `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, and `natsMessageQueueAccount` parameters, make sure that all these parameters are specified in the response file.

   If the response file does not exist, create a new response file that contains the parameters for connecting Kaspersky Security Center Web Console to Administration Server. Name the file ksc-web-console-setup.json, and then place it in the /etc directory.

   **Example of a response file containing the minimum set of parameters**

The set of parameters of the response file depends on the version of the Administration Server to which the Kaspersky Security Center Web Console connects:

- Administration Server version 16 or later

  Example of a response file with the minimum set of parameters for signing in to Administration Server version 16 or later:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Administration Server version 15.4 or later

  Example of a response file with the minimum set of parameters for signing in to Administration Server version 15.4 or earlier:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

You can install Kaspersky Security Center Web Console either on the same device as Administration Server or on a different device. If Kaspersky Security Center Web Console is installed on a different device, the Kaspersky Security Center Web Console address (specified by `address`) and the Administration Server address (specified by `iamHost` or `kscHost`) differ. If Kaspersky Security Center Web Console is installed on the same device as Administration Server, these parameters have the same values.

The `iamHost` value must match the IAM address that you specified when installing Administration Server. To obtain the specified IAM address, run the following command on the device with Administration Server installed:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

For detailed information, refer to the article: Kaspersky Security Center Web Console installation parameters.

You can add multiple Administration Servers of different versions to the list of trusted servers. In this case, the Servers may use different authentication methods.

If you want to upgrade Kaspersky Security Center Web Console connected to Administration Server installed on the Kaspersky Security Center Linux failover cluster nodes, in the response file, specify the trusted installation parameter to allow the Kaspersky Security Center Linux failover cluster to connect to Kaspersky Security Center Web Console.

Components of the `trusted` **installation parameter**

If you connect to the Kaspersky Security Center Linux failover cluster by using domain authentication with SSO, specify the trusted installation parameter as follows: If you connect Kaspersky Security Center Web Console to Administration Server version 16 or later, domain authentication with single sign-on (SSO) provided by Identity and Access Manager (IAM) will be used. In this case, specify the `trusted` installation parameter as follows:

```
"trusted":  {
  "<Administration Server name>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<shared data folder>/iam/main_certificate.pem",
    "iamPATPath": "<shared data folder>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<shared data folder>/1093/cert/klserver.cer"
  }
}
```

where:

- `<Administration Server name>` is the Kaspersky Security Center Linux failover cluster name that will be displayed in the login window of Kaspersky Security Center Web Console.

- `iamHost` is the address of the device where Administration Server and IAM are installed. If you created a secondary network adapter when preparing the cluster nodes, use the FQDN or host name of the adapter as the Kaspersky Security Center Linux failover cluster address. Otherwise, specify the FQDN or host name of the third-party load balancer that you use.

  The `iamHost` value must match the IAM address specified when installing the Administration Server. To obtain the specified IAM address, run the following command on the device with Administration Server installed:

  `grep "iam_address:" <shared data folder>/iam/iam_config.yaml`

- `iamOAuthPort` is the port that is used for exchanging authentication tokens over the OpenID Connect authentication protocol (default value is 4444). This port is used both for communication between Kaspersky Security Center Web Console Server and Administration Server, and between the browser (used with Kaspersky Security Center Web Console) and Administration Server.

- `iamProxyPort` is the port that is used for connecting Kaspersky Security Center Web Console Server to Administration Server (default value is 9050).

- `iamCertPath` is the path to the IAM certificate. The IAM certificate is created automatically the first time you run Administration Server. The certificate is located on the device where Administration Server is installed. The default path to the certificate is: `<shared data folder>/iam/main_certificate.pem`. The certificate is located in the shared data storage of the Kaspersky Security Center Linux failover cluster. The self-signed IAM certificate is rotated automatically.

- `iamPATPath` is the path to the token used for registration of Kaspersky Security Center Web Console as an OAuth-client in IAM. This file is generated automatically the first time you run Administration Server. The token is located on the device where Administration Server is installed. The default path to the token is: <shared data folder>/iam/initial_token.txt. The token is located in the shared data storage of the Kaspersky Security Center Linux failover cluster. The token is valid indefinitely and does not require rotation.

- `kscPort` is the OpenAPI port that Kaspersky Security Center Web Console use to connect to Administration Server (default value is 13299).

- `kscCertPath` is the Administration Server certificate that is located in the shared data storage of the Kaspersky Security Center Linux failover cluster. The default path to the certificate file is: `<shared data folder>\1093\cert\klserver.cer`.

  Copy the Administration Server certificate file (specified by `kscCertPath`), the IAM certificate file (specified by `iamCertPath`), and the token file (specified by `iamPATPath`) from the shared data storage to the device where you install Kaspersky Security Center Web Console. Specify the local path to the Administration Server certificate.

If you connect Kaspersky Security Center Web Console to Administration Server version 15.4 or earlier, authentication by specifying the name and password of the domain user or the internal user will be used. In this case, specify the trusted installation parameter as follows:

```
"trusted":  {
  "<Administration Server name>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<shared data folder>/1093/cert/klserver.cer"
  }
}
```

where:

- `<Administration Server name>` is the Kaspersky Security Center Linux failover cluster name that will be displayed in the login window of Kaspersky Security Center Web Console.
- `kscHost` is the Administration Server address (FQDN or host name). If you created a secondary network adapter when preparing the cluster nodes, use the address of the adapter as the Kaspersky Security Center Linux failover cluster address. Otherwise, specify the address of the third-party load balancer that you use.
- `kscPort` is the OpenAPI port that Kaspersky Security Center Web Console uses to connect to Administration Server (default value is 13299).
- `kscCertPath` is the Administration Server certificate that is located in the shared data storage of the Kaspersky Security Center Linux failover cluster. The default path to the certificate file is: `<shared data folder>\1093\cert\klserver.cer`. Copy the certificate file from the shared data storage to the device where you install Kaspersky Security Center Web Console. Specify the local path to the Administration Server certificate.

Kaspersky Security Center Web Console cannot be upgraded by using the same installation file. If you want to change the settings in a response file and use this file to reinstall the application, you must first remove the application, and then install it again with the new response file.

4. Under an account with root privileges, use the command line to run the setup file with the .deb or .rpm extension, depending on your Linux distribution.

   To upgrade from a previous version of Kaspersky Security Center Web Console, run one of the following commands:

   - For devices running an RPM-based operating system:
     `sudo yum install ksc-web-console-<build_number>.x86_64.rpm`
   - For devices running a Debian-based operating system:
     `sudo apt-get install ksc-web-console-<build_number>.x86_64.deb`

   This starts unpacking of the setup file. Please wait until the installation is complete.

5. Restart all of the Kaspersky Security Center Web Console services by running the following command:
   `sudo systemctl restart KSC*`

   When the upgrade is complete, you can use your browser to open and log in to Kaspersky Security Center Web Console.

# Upgrading Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode

This article describes how to upgrade Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) on the Astra Linux Special Edition operating system.

*To upgrade Kaspersky Security Center Web Console:*

1. Make sure that the device on which you want to upgrade Kaspersky Security Center Web Console is running one of the supported Linux distributions.

2. Read and accept the End User License Agreement (EULA). If the Kaspersky Security Center Linux distribution kit does not include a TXT file with the text of EULA, you can download the file from the Kaspersky website. If you do not accept the terms of the License Agreement, do not upgrade Kaspersky Security Center Web Console by using the installation file.

3. Use the same response file that you prepared before installing Kaspersky Security Center Web Console. The response file name is ksc-web-console-setup.json. The file location is /etc/ksc-web-console-setup.json.

   If the response file does not exist, create a new response file that contains the parameters for connecting Kaspersky Security Center Web Console to Administration Server. Name the file ksc-web-console-setup.json, and then place it in the /etc directory.

   **Example of a response file containing the minimum set of parameters**

   The set of parameters of the response file depends on the version of the Administration Server to which the Kaspersky Security Center Web Console connects:

   - Administration Server version 16 or later

     Example of a response file with the minimum set of parameters for signing in to Administration Server version 16 or later:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Administration Server version 15.4 or later

  Example of a response file with the minimum set of parameters for signing in to Administration Server version 15.4 or earlier:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

You can install Kaspersky Security Center Web Console either on the same device as Administration Server or on a different device. If Kaspersky Security Center Web Console is installed on a different device, the Kaspersky Security Center Web Console address (specified by `address`) and the Administration Server address (specified by `iamHost` or `kscHost`) differ. If Kaspersky Security Center Web Console is installed on the same device as Administration Server, these parameters have the same values.

The `iamHost` value must match the IAM address that you specified when installing Administration Server. To obtain the specified IAM address, run the following command on the device with Administration Server installed:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

For detailed information, refer to the article: Kaspersky Security Center Web Console installation parameters.

You can add multiple Administration Servers of different versions to the list of trusted servers. In this case, the Servers may use different authentication methods.

4. Ensure that in the `/etc/digsig/digsig_initramfs.conf` file, the `DIGSIG_ELF_MODE` parameter is specified as follows:

   ```
   DIGSIG_ELF_MODE=1
   ```

5. Ensure that the `astra-digsig-oldkeys` compatibility package is installed.

   If this package is not installed, run the following command:

   ```
   apt install astra-digsig-oldkeys
   ```

6. Create a directory for the application key, if it does not exist:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. Place the application key /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg in the directory created in the previous step:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   If the Kaspersky Security Center Linux distribution kit does not include the kaspersky_astra_pub_key.gpg application key, you can download it by clicking the link: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Update the RAM disks:

   ```
   update-initramfs -u -k all
   ```

Reboot the system.

9. Under an account with root privileges, use the command line to run the setup file. You receive the installation file by downloading it from the Kaspersky website.

   To upgrade from a previous version of Kaspersky Security Center Web Console, run the following command:

   ```
   sudo apt-get install ksc-web-console-<build_number>.x86_64.deb
   ```

   This starts unpacking of the setup file. Please wait until the installation is complete.

10. Restart all of the Kaspersky Security Center Web Console services by running the following command:

    ```
    sudo systemctl restart KSC*
    ```

When the upgrade is complete, you can use your browser to open and log in to Kaspersky Security Center Web Console.

# Migration to Kaspersky Security Center Linux

Use the **Scenario for migration to Kaspersky Security Center** if all the conditions are satisfied:

- You do not need to install the Administration Server and the DBMS on separate devices.
- The operating system for the Administration Server is Ubuntu, Astra Linux, CentOS, or RED OS.
- PostgreSQL is suitable for the new Administration Server.
- The old Administration Server used PostgreSQL or Microsoft SQL Server as the DBMS.

Select **General guide for migration to a new Kaspersky Security Center Linux server** if at least one of the conditions is satisfied:

- You need to install the Administration Server and the DBMS on separate devices.
- The new Administration Server must use a non-PostgreSQL DBMS.
- The operating system for the Administration Server is not Ubuntu, Astra Linux, CentOS, or RED OS.

Select **Migration to Kaspersky Security Center by using the Migration wizard** if:

- The DBMS type for the old Kaspersky Security Center Administration Server is different from the new server, and Microsoft SQL Server is not used.
- You have experience with switching managed devices to the new Administration Server using Kaspersky Security Center tasks and utilities.

Please refer to the manuals for details on special considerations and limitations.

# General guide for migration to a new Kaspersky Security Center Linux server

You can use a backup copy of data to migrate data from a Kaspersky Security Center Windows or Kaspersky Security Center Linux Administration Server to a new Kaspersky Security Center Linux server when migrating the solution or replacing hardware.

Before migrating data from Kaspersky Security Center Windows, make sure that the necessary features of Kaspersky Security Center Windows are supported by Kaspersky Security Center Linux.

The general migration guide considers the scenario in which the new Administration Server gets a new DNS name. To restore the connection of managed devices, you need to change the DNS record of the old server. If you have sufficient experience in configuring the solutions, you can devise your own scenario for assigning the old address to the new server during installation. The presence of the old Administration Server is on the network may cause device management faults and interfere with the logon process in the Web Console of the new Administration Server; it can also make the Network Agent installation task connect to the old server.

Limitations

- The migration can be performed between the following DBMSs:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- You need to specify the target DBMS type in the backup utility when migrating from Microsoft SQL Server; in other migration scenarios, the compatibility of databases is determined by the paragraph above.
- The version of the DBMS on the new Administration Server must not be older than the version of the DBMS used on the previous Administration Server.
- Kaspersky Security Center Windows must be updated to the latest version before creating a backup copy for data migration.
- If you use MySQL or MariaDB as a DBMS for Kaspersky Security Center Windows and for Kaspersky Security Center Linux, the `lower_case_table_names` parameter must match for the current and new DBMSs.

## 1 Preparing to create a backup copy

This step contains instructions for preparing a previously configured Administration Server to subsequent migration to the new Kaspersky Security Center Linux Administration Server. The preliminary steps are as follows:

1. Check the version of the Administration Server to create a backup copy compatible with Kaspersky Security Center Linux.

   All current versions of **Kaspersky Security Center Linux** support data migration when upgrading to a newer version of the application. Backup copies can be created and restored only within one type of DBMS.

   For **Kaspersky Security Center Windows**, check the version of the Administration Server in **Properties** → **General** → **Version**. If the version is earlier than 15.1.0.22239, upgrade Kaspersky Security Center Windows to the latest version.

   **Upgrading Kaspersky Security Center Windows to the latest version**

   1. From the Kaspersky website, download the distribution package corresponding to the localization language of your installed Administration Server: `Version 15.1.0.22239 | Windows | Full distributive`.

      The executable file is saved to your **Downloads** folder with the following name: `ksc_15.1_<build number>_full_<language>.exe`.

   2. Copy the distribution package to the Administration Server.

3. Run the `ksc_15.1_<build number>_full_<language>.exe` executable file as administrator.

4. In the displayed window, click the **Install Kaspersky Security Center** link.

   The Administration Server Setup wizard starts.

5. Read the License Agreement and Privacy Policy. If you agree with all the terms and conditions of the End User License Agreement and the Privacy Policy, select the following check boxes under **I confirm that I have fully read, understand, and accept the terms and conditions of the following**:

   - **The terms and conditions of this EULA**.
   - **Privacy Policy describing the handling of data**.

6. Select **Upgrade Administration Server and web-based console (recommended)** and go to the next step.

7. Create a new backup copy by selecting **I want to create a backup copy of data** and completing the backup wizard.

8. Click **Upgrade**.

9. During the upgrade, in the Web Console setup wizard, confirm all steps of the wizard to upgrade the version.

   The upgrade process takes some time. After the setup wizard has finished, the Administration Console may not accept connections until the database is initialized.

10. Wait until the upgrade is complete.

2. Check the Administration Server certificate for compliance.

   Before creating a backup copy, make sure that the certificate contains the Subject Alternative Name (SAN). If not, it is important to replace the certificate, otherwise you will not be able to log in to the Web Console after restoring from a backup copy.

   *To verify that the certificate includes a Subject Alternative Name*:

   - For a Windows-based device:

     a. In the Administration Console, select the Administration Server that you want to check.

     b. In the context menu, select **Properties** → **General** → **View Administration Server certificate**.

     c. In the displayed window, check the **Subject Alternative Name** value.

   - For a Linux device, run the following command:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   Make sure that the Subject Alternative Name contains the domain name (DNS) of the Administration Server host.

   If the value contains only an IP address, or the value is missing altogether, manually replace the certificate with a certificate that meets the requirements for working with Kaspersky Security Center Linux. Replace the Administration Server general certificate by using the klsetsrvcert utility.

### Replacing the Administration Server general certificate by using the klsetsrvcert utility

1. Create a new certificate with a delayed start date of use on devices by running the following command:

   - For Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
     <oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   - For Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   where `"<oldksc.example.internal>"` is the FQDN of the connection to the Administration Server.

   > Do not use an IP address for this value.

2. Set the start date for the new certificate on all hosts by running the following command:

   - For Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

   - For Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
     ```

   where the `"DD-MM-YYYY hh:mm"` date is at least 30 days after the current date. By default, the distribution period for a new certificate (`CR`) is 90 days.

   > When the configured time comes, you will need to reinstall the Web Console to restore access to it and have its certificate actualized.

3. If necessary, after migration to a new Administration Server, run the klmover utility to restore the connection of hosts to the Administration Server. You may need to run the utility if the host has been powered off for the entire certificate distribution period or if it has not connected to the Administration Server.

## 2 Creating a backup copy of the old installation of the Administration Server

### Creating a backup copy of Kaspersky Security Center Windows

1. From the menu **Start** → **Kaspersky Security Center** → **Kaspersky Backup Utility**, run the `klbackup.exe` utility from the Kaspersky Security Center Linux installation folder.

   The Setup Wizard starts. On Microsoft Windows in Server Core mode, use the console version of the klbackup utility.

2. At the first step, select **Perform backup of Administration Server data**.

3. At the **Backup settings** step:

   a. Click the **Browse** button and create a new folder to save the backup copy away from the default directory, for example `C:\kscbackups`.

   b. If you are using Microsoft SQL Server, select the **Database migration → Migrate to Postgres format** option for use with the quick install script. With the usual method of deploying Kaspersky Security Center Linux, you can also migrate data to a MySQL/MariaDB database.

   c. Set a password for the backup copy to protect data from unauthorized access.

4. Wait for the backup copy to be created and exit the utility.

A new directory is created in the directory with the timestamp of the backup copy.

**Creating a backup copy of Kaspersky Security Center Linux**

1. On the Administration Server device, enter the following command on the command line:

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. Wait until the backup copy is created.

In the directory specified in `-path`, a new directory is created with the timestamp of the backup copy.

After creating a backup copy of the old Administration Server, decommission the device with the Administration Server.

**Decommissioning the Administration Server device**

1. Copy the resulting backup copy to transfer data to the administrator's workstation.

2. Shut down the operating system of the Administration Server.

3. Disconnect the network adapter from the corporate network.

4. Release the IP address of the device if you want to use it for the new installation of Kaspersky Security Center Linux.

5. Make sure the device is completely disconnected.

The presence of the old Administration Server is on the network may cause device management faults and interfere with the logon process in the Web Console of the new Administration Server; it can also make the Network Agent installation task connect to the old server.

3 Initial installation of Kaspersky Security Center Linux

- **Preparation for deployment**

  Before proceeding with the installation, prepare the following:

  - The installation disk image of the operating system and the application package repository.
  - An authenticator application for two-factor authentication (2FA) when logging in to the Web Console.
  - New FQDN (for example, *ksclinux.example.com*). If you have sufficient experience in configuring the solutions, you can devise your own scenario for assigning the old FQDN to the new server during installation. In this case, at step 5 "Configuring the application after restoring from a backup copy", skip step 4. "Restoring the connection of managed devices to the FQDN of the previous Administration Server".
  - The administrator's workstation with a browser for internet access to download distribution packages and manage the Web Console.
  - Make sure the DNS server and the time server (NTP) are available for application components.
  - Depending on the scenario, release the old IP address if an IP address was used for managed device connections.
  - Configure network equipment and the proxy server in accordance with the requirements:
    - Ports for communication of application components.
    - Access to Kaspersky servers.
    - Hardening Guide.

- **Choosing a configuration, configuring and installing**

  a. Prepare the equipment for the Administration Server, DBMS, and Web Console in accordance with the hardware and software requirements and calculated hardware resources to allow for the management of the required number of devices under the design load.

  To improve the security of the solution components, include the Kaspersky Endpoint Security for Linux application in the sizing calculations and install it on the Kaspersky Security Center Linux nodes.

  b. Install and configure the operating system and components of the Kaspersky Security Center solution in accordance with the instructions for the initial deployment of the solution.

- **Logging in to the Web Console for the first time**

  1. In your browser, open the address for connecting to the Web Console: `https://<FQDN>:8080`

     where `<FQDN>` is the Administration Server address from the script installation settings, for example, *https://ksclinux.example.com:8080*.

  2. To log in to the Web Console, use the user name and password from the script output.

3. Configure the authenticator application:

   a. Copy the secret key for getting one-time codes to the application or scan the QR code from the Web Console authentication configuration wizard.

   b. Enter the generated code to authenticate and log in to the Web Console.

4. Review and confirm that you have read the Hardening Guide.

5. Configure the Administration Server in the quick start wizard if you do not intend to restore Administration Server data from a backup copy.

## 4 Restoring from a backup copy of Administration Server

Restoring from a backup copy of Administration Server involves the following steps:

**1. Transferring the backup copy to the Administration Server**

Transfer the backup copy of the old Administration Server to the new Administration Server device using removable media or over the network.

*To transfer the backup copy to the Administration Server over the network:*

> Whether you can use the scp utility to copy the data depends on the whether the SSH service is installed and running in the operating system of the Administration Server device and the security policy of your organization.

1. On the command line of the device, use the *cd* command to change to the directory containing the files of the backup copy of the old Administration Server, for example:

   Windows

   ```
   cd C:\kscbackups
   ```

   Linux

   ```
   cd /root/kscbackups
   ```

2. Copy the directory containing the files of the backup copy using the scp utility:

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   where:

   `<klbackup202x-xx-xx>` is the directory with the files of the backup copy.

   `<administrator>` is the privileged user on the new Administration Server with SSH connection rights.

   `<ksclinux.example.com>` is the FQDN of the new Administration Server.

The directory with the backup copy is copied to specified user's home directory.

### 2. Procedure for restoring from a backup copy

1. On the new Administration Server device, open the command line.
2. While you are restoring data from a backup copy, temporarily grant PostgreSQL superuser rights to the standard klserver and kliam accounts that the Administration Server uses to connect to the DBMS:

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
   ```

3. Use the klbackup utility to start data restoration from the backup copy of the old Administration Server:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
   ```

   where `</home/administrator/klbackup202x-xx-xx>` is the full path to the directory containing the files of the backup copy.
4. If no password has been set for the backup copy, when prompted for the backup copy password, press **Enter** without entering a password.
5. Wait until the utility finishes.

   Large installations can take a long time.
6. Restore the original rights of the PostgreSQL accounts that the Administration Server uses to connect to the DBMS.

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
   ```

## 5 Configuring the application after restoring from a backup copy

Skip this step if you did not restore data from a backup copy.

The procedure for configuring the application after restoring from a backup copy involves the following steps:

### 1. Restoring the Web Console

1. Get the address of the old server from the IAM Server configuration file:

   ```
   sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

   Example

   ```
   ksc_address: "oldksc.example.internal"
   ```

2. Verify that the FQDN address of the old Administration Server is being converted correctly to the loopback IP address of the new Administration Server. To do this:

   a. Run the `ping` command with the address of the old Administration Server.

   Example of successfully getting a loopback IP address

   ```
   administrator@ksclinux:~$ ping oldksc.example.internal
   ping oldksc.example.internal
   PING ksclinux (127.0.1.1) 56(84) bytes of data.
   64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
   ```

   b. Add the address of the old Administration Server to the `[[/etc/hosts]]` file of the operating system of the new Administration Server, if the address was not obtained or if an external IP address was obtained. To do this:

   - Open /etc/hosts for editing:

     ```
     sudo nano /etc/hosts
     ```

   - Enter the name of the old server as an additional alias for the Administration Server device address.

     Example

     ```
     127.0.0.1       localhost
     127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
     <...>
     ```

3. Reinstall the Web Console.

   a. Delete the local Web Console Server:

   Depending on your Kaspersky Security Center Linux distribution, run one of the following commands:

   - For a device running a Debian-based operating system:

     ```
     sudo apt remove ksc-web-console -y
     ```

   - For a device running a Red Hat Enterprise Linux-based operating system:

     ```
     sudo dnf remove ksc-web-console -y
     ```

   b. Start the installation of the Web Console package from the directory with distribution packages:

   - On a device running a Debian-based operating system:

     ```
     sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
     ```

   - For a device running a Red Hat Enterprise Linux-based operating system:

     ```
     sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
     ```

**2. Restoring kscadmin user access for migration from Kaspersky Security Center Windows**

The user database has been overwritten; create the kscadmin user and configure two-factor authentication from scratch.

1. Open the command line in the operating system of the Administration Server device and run the following command to create a user:

   ```
   sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
   ```

   After pressing **Enter**, set a password, then re-enter the password.

2. In your browser, open the address for connecting to the Web Console:

   ```
   https://<FQDN>:8080
   ```

   where `<FQDN>` is the Administration Server address from the script installation settings, for example, *https://ksclinux.example.com:8080*.

3. Use the generated user name and password to log in to the Web Console.

4. Configure an authenticator application. To do this:

   a. Delete the old kscadmin user account profile that was configured in your authenticator application before you began restoring the backup copy of the Administration Server.

   b. Copy the secret key for getting one-time codes to the application or scan the QR code from the Web Console authentication configuration wizard.

   c. Enter the generated code to authenticate and log in to the Web Console.

**3. Testing the Administration Server**

1. Test the Web Console interface as the kscadmin user and other users.

2. Run the following tasks in sequence:

   - Download updates to the Administration Server repository
   - Administration Server maintenance
   - Backup of Administration Server data

   Replace the Windows paths in the task settings with Linux paths of the new Administration Server, or delete the tasks and configure new tasks from scratch.

3. Review the results of the tasks and, if necessary, make changes to the settings of the tasks, management policies and Administration Server settings.

**4. Restoring the connection of managed devices to the FQDN of the previous Administration Server**

If you assigned a new FQDN address to the new Administration Server (for example, ksclinux.example.com), add one of the following types of DNS records:

- A CNAME record mapping the old Administration Server name to the new Administration Server name.

  For more information about configuring the required records, refer to your DNS server documentation.

- An A and AAAA record for the old Administration Server address pointing to the new Administration Server IP address.

  For a DNS service based on Windows Server, run commands with values that are applicable to your infrastructure.

*To add a DNS A record for a DNS service based on Windows Server, run the commands using values that are applicable to your infrastructure:*

1. Connect to the DNS server.
2. Open PowerShell and get the IP address from the existing A record by running the following command:

   ```
   Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
   ```

3. Change the IP address in the A record by running the following commands:

   ```
   $OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
   ```

   ```
   $NewKSC = $OldKSC.Clone()
   ```

   ```
   $NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
   ```

   ```
   Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
   ```

4. Make sure the IP address in the A record has been updated by running the following command:

   ```
   Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
   ```

   The command output displays the IP address of the Kaspersky Security Center Linux Administration Server. Managed devices will restore their connections after updating the local DNS cache.

## 6 Configuring Anti-Virus protection of the Administration Server

To implement the Anti-Virus protection guidelines of the Hardening Guide on the Administration Server, install Kaspersky applications on the Administration Server and configure management policies for the installed applications.

Installation and configuration involves the following steps:

**1. Creating a separate administration group**

1. In the main window of the Web Console, select **Asset management** → **Hierarchy of groups**.
2. Select the check box next to the **Managed devices** group.
3. Click **Add**.
4. In the displayed window, enter a name for the new group (for example, *kscserver*) and confirm its creation by clicking the **Add** button.

**2. Creating a policy for the Network Agent without inheritance of settings**

1. In the main window of the Web Console, go to the **Asset management** → **Policies** section.
2. Then click the **Add** button.
3. In the New policy wizard, select the **Kaspersky Security Center Linux Network Agent** application and click **Next**.
4. Disable the **Inherit settings from parent policy** option and click **Save**.

**3. Installing the Kaspersky Endpoint Security for Linux management plug-in from Kaspersky Security Center Linux or manually**

You can install the management plug-in for Kaspersky Endpoint Security for Linux in the following ways:

- From the list of available distribution packages in the Web Console
- Manually from a file

*To install the Kaspersky Endpoint Security management plug-in from the list of available distribution packages in the Web Console:*

1. In the main window of the Web Console, select **Settings** → **Web plug-ins**.

   This opens the list of installed web plug-ins.
2. Then click the **Add** button.

   The list of available management plug-ins is displayed. This list is automatically updated whenever a new version of a web plug-in is released.
3. In the list of available plug-ins, select the latest available version of the Kaspersky Endpoint Security for Linux web plug-in.
4. In the displayed web plug-in description window, click the **Install plug-in** button.
5. Wait until the installation is complete and click the **OK** button in the information window.

The new plug-in is added to the list of installed web plug-ins.

*Video: installing the web plug-in using the wizard*




*To install the Kaspersky Endpoint Security management plug-in manually from a file:*

1. Download the archive with the web plug-in from the application download page in the Kaspersky Endpoint Security for Linux section: **Application Control plug-in** → **Web console Plug-In**.
2. Unpack the downloaded archive locally.
3. In the main window of the Web Console, select **Settings** → **Web plug-ins**.

   This opens the list of installed web plug-ins.
4. Click the **Add from file** button.
5. In the displayed window, enter the path to the plugin.zip file and the path to the signature.txt file.

   These files are located in the folder in which unpacked the archive with the web plug-in.
6. Then click the **Add** button.
7. Wait until the installation is complete and click the **OK** button in the information window.

The new plug-in appears in the list of installed web plug-ins (**Settings** → **Web plug-ins**).

*Video: installing the management web plug-in in isolated networks*



### 4. Creating a policy for Kaspersky Endpoint Security for Linux without inheritance of settings

When using Kaspersky Endpoint Security for Linux together with Kaspersky Security Center Linux, you need to configure the policy in accordance with the recommendations of Kaspersky experts.

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Select an administration group for the Administration Server.
3. Click **Add**.

   The New policy wizard starts.
4. In the displayed window, select the Kaspersky Endpoint Security for Linux application from the list.
5. Specify the **Standard mode or the Kaspersky Endpoint Detection and Response Agent mode** for Kaspersky Endpoint Security for Linux.
6. Make a decision about using Kaspersky Security Network.
7. Review the optimization guidelines for managed devices.
8. In the name of the policy, indicate that the policy belongs to the Administration Server.
9. Disable the **Inherit settings from parent policy** option.
10. Save your changes.

*Video: creating a policy*




### 5. Creating an Update group task for Kaspersky Endpoint Security for Linux

1. In the main window of the Web Console, select the **Tasks** section.
2. Select an administration group for the Administration Server.
3. Click **Add**.

   The New task wizard starts.
4. In the displayed window, select the Kaspersky Endpoint Security for Linux application from the list.

5. Specify the *Update* task type and click through the next steps without changing any settings.

   This opens the task properties window.

6. In the **Application settings** → **Sources of updates** section, enable the Kaspersky Security Center source and raise its priority.

In an isolated network, use the Kaspersky Update Utility to create a repository for update tasks.

*Video: configuring centralized database updates*




**6. Adding a license key to the Administration Server repository with automatic distribution**

1. In the main window of Kaspersky Security Center Web Console, select the **Licenses** section.
2. Click **Add**.
3. Select the **Activation code** option and click **Send**.

   In an isolated network, use a key file that you can request using the service at https://keyfile.kaspersky.com/en.
4. In the list of licenses, click the name of the license.
5. Select the **Automatically distribute license key to managed devices** check box.
6. Save your changes.

*Video: activating the application with an activation code*




*Video: activating the application with a key file*




**7. Creating installation packages for the Network Agent and Kaspersky Endpoint Security for Linux**

1. In the main window of the Web Console, select **Software management** → **Installation packages**.
2. Click **Add**.
   The New package wizard starts.
3. Select **Create an installation package for a Kaspersky application**.
4. In the list of applications, find the latest version of Kaspersky Endpoint Security for Linux and click its name.
5. In the sidebar, start the download by clicking the **Download and create installation package** button.
   Review and accept the license agreements to start using the applications.

6. Return to the list of applications and download the latest version of the Kaspersky Network Agent for Linux.

   Review and accept the license agreements to start using the applications.

7. In the main window of the Web Console, in the list of downloaded applications, click the names of the applications.

In an isolated network, download the distribution packages from the Kaspersky website and in the New package wizard, select the **Create an installation package from a file** option.

*Video: automatic creation of an installation package in Kaspersky Security Center*




*Video: manual creation of an installation package from a file in Kaspersky Security Center*




**8. Installing Network Agent for Linux**

1. In the main window of the Web Console, select **Software Management** → **Installation packages**.
2. Select the check box next to the **Kaspersky Network Agent for Linux** package.
3. Click **Deploy**.

   The Protection deployment wizard starts.

4. Select the **Using a stand-alone package** option.

5. At the **Move devices to the Managed devices folder** step, skip configuring the rules for moving devices to an administration group. This option is not applicable to the Administration Server device.

6. At the **Result of stand-alone installation package creation** step, select and copy the full path to the application installation script.

7. Open the command line of the operating system of the Administration Server.

8. Start the installation of the stand-alone package:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   where `</var/opt/.../stand-alone_package_sh>` is the previously copied full path to the script file of the stand-alone installation package.

   If the installation is successful, a notification is displayed to that effect.

9. Move the Administration Server device (for example, *ksclinux*) from the **Managed devices** group to the previously prepared administration group (for example, *kscserver*).

**9. Installing Kaspersky Endpoint Security for Linux**

1. In the main window of the Web Console, select **Software Management** → **Installation packages**.

2. Select the check box for the Kaspersky Endpoint Security for Linux package.

3. Click **Deploy**.

   The Protection deployment wizard starts.

4. Select the **Using a stand-alone package** option.

5. At the **Result of stand-alone installation package creation** step, select and copy the full path to the application installation script.

6. Open the command line of the operating system of the Administration Server.

7. Start the installation of the stand-alone package:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   where `</var/opt/.../stand-alone_package_sh>` is the previously copied full path to the script file of the stand-alone installation package.

   If the installation is successful, a notification is displayed to that effect.

8. In the main window of the Web Console, in the **Tasks** section, select the root node in the list of administration groups with the name of the Administration Server.

9. From the list of Administration Server tasks, start the following tasks in sequence:

   - "Download updates to the Administration Server repository"
   - Update (Kaspersky Endpoint Security for Linux)

10. In the main window of the Web Console, select **Asset management** → **Managed devices**.

11. Click the name of the Administration Server device object.

12. Review the values of the main indicators of the device status:

    - Anti-virus databases last updated (up-to-date)
    - Connected to Administration Server (up-to-date)
    - Protection status (Running)
    - *Key added successfully* event (present)

Follow the Kaspersky Endpoint Security for Linux deployment scenario to deploy the application to devices on your network.

# Scenario for migration to Kaspersky Security Center Linux using the quick installation script.

The scenario includes examples of migrating the solution with its data to a new Administration Server device to:

- Migrate from Kaspersky Security Center Windows (MS SQL or PostgreSQL) to Kaspersky Security Center Linux (PostgreSQL).
- Migrate Kaspersky Security Center Linux (PostgreSQL) for hardware replacement.

Deploying a new Administration Server involves using the quick installation script.

Other methods of data migration are described in the Migration to Kaspersky Security Center Linux article.

## 1 Preparing to create a backup copy

This step contains instructions for preparing a previously configured Administration Server to subsequent migration to the new Kaspersky Security Center Linux Administration Server. The preliminary steps are as follows:

1. Check the version of the Administration Server to create a backup copy compatible with Kaspersky Security Center Linux.

   All current versions of **Kaspersky Security Center Linux** support data migration when upgrading to a newer version of the application. Backup copies can be created and restored only within one type of DBMS.

   For **Kaspersky Security Center Windows**, check the version of the Administration Server in **Properties** → **General** → **Version**. If the version is earlier than 15.1.0.22239, upgrade Kaspersky Security Center Windows to the latest version.

   **Upgrading Kaspersky Security Center Windows to the latest version**

   1. From the Kaspersky website, download the distribution package corresponding to the localization language of your installed Administration Server: `Version 15.1.0.22239 | Windows | Full distributive`.

      The executable file is saved to your **Downloads** folder with the following name: `ksc_15.1_<build number>_full_<language>.exe`.

2. Copy the distribution package to the Administration Server.

3. Run the `ksc_15.1_<build number>_full_<language>.exe` executable file as administrator.

4. In the displayed window, click the **Install Kaspersky Security Center** link.

   The Administration Server Setup wizard starts.

5. Read the License Agreement and Privacy Policy. If you agree with all the terms and conditions of the End User License Agreement and the Privacy Policy, select the following check boxes under **I confirm that I have fully read, understand, and accept the terms and conditions of the following**:

   - **The terms and conditions of this EULA**.
   - **Privacy Policy describing the handling of data**.

6. Select **Upgrade Administration Server and web-based console (recommended)** and go to the next step.

7. Create a new backup copy by selecting **I want to create a backup copy of data** and completing the backup wizard.

8. Click **Upgrade**.

9. During the upgrade, in the Web Console setup wizard, confirm all steps of the wizard to upgrade the version.

   The upgrade process takes some time. After the setup wizard has finished, the Administration Console may not accept connections until the database is initialized.

10. Wait until the upgrade is complete.

2. Check the Administration Server certificate for compliance.

   Before creating a backup copy, make sure that the certificate contains the Subject Alternative Name (SAN). If not, it is important to replace the certificate, otherwise you will not be able to log in to the Web Console after restoring from a backup copy.

   *To verify that the certificate includes a Subject Alternative Name*:

   - For a Windows-based device:

     a. In the Administration Console, select the Administration Server that you want to check.

     b. In the context menu, select **Properties** → **General** → **View Administration Server certificate**.

     c. In the displayed window, check the **Subject Alternative Name** value.

   - For a Linux device, run the following command:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   Make sure that the Subject Alternative Name contains the domain name (DNS) of the Administration Server host.

   If the value contains only an external IP address without a domain name (DNS), or the value is missing altogether, manually replace the certificate with a certificate that meets the requirements for working with Kaspersky Security Center Linux. Replace the Administration Server general certificate by using the klsetsrvcert utility.

#### Replacing the Administration Server general certificate by using the klsetsrvcert utility

1. Create a new certificate with a delayed start date of use on devices by running the following command:

   - For Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
     <oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   - For Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
     ```

   where `"<oldksc.example.internal>"` is the FQDN of the connection to the Administration Server.

   > Do not use an IP address for this value.

2. Set the start date for the new certificate on all hosts by running the following command:

   - For Kaspersky Security Center Windows:

     ```
     "%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
     ```

   - For Kaspersky Security Center Linux:

     ```
     /opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
     ```

   where the `"DD-MM-YYYY hh:mm"` date is at least 30 days after the current date. By default, the distribution period for a new certificate (`CR`) is 90 days.

   > When the configured time comes, you will need to reinstall the Web Console to restore access to it and have its certificate actualized.

3. If necessary, after migration to a new Administration Server, run the klmover utility to restore the connection of hosts to the Administration Server. You may need to run the utility if the host has been powered off for the entire certificate distribution period or if it has not connected to the Administration Server.

## 2 Creating a backup copy of the old installation of the Administration Server

#### Creating a backup copy of Kaspersky Security Center Windows

1. From the menu **Start** → **Kaspersky Security Center** → **Kaspersky Backup Utility**, run the `klbackup.exe` utility from the Kaspersky Security Center Linux installation folder.

   The Setup Wizard starts. On Microsoft Windows in Server Core mode, use the console version of the klbackup utility.

2. At the first step, select **Perform backup of Administration Server data**.

3. At the **Backup settings** step:

   a. Click the **Browse** button and create a new folder to save the backup copy away from the default directory, for example `C:\kscbackups`.

   b. If you are using Microsoft SQL Server, select the **Database migration → Migrate to Postgres format** option for use with the quick install script. With the usual method of deploying Kaspersky Security Center Linux, you can also migrate data to a MySQL/MariaDB database.

   c. Set a password for the backup copy to protect data from unauthorized access.

4. Wait for the backup copy to be created and exit the utility.

A new directory is created in the directory with the timestamp of the backup copy.

**Creating a backup copy of Kaspersky Security Center Linux**

1. On the Administration Server device, enter the following command on the command line:

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. Wait until the backup copy is created.

In the directory specified in `-path`, a new directory is created with the timestamp of the backup copy.

After creating a backup copy of the old Administration Server, decommission the device with the Administration Server.

**Decommissioning the Administration Server device**

1. Copy the resulting backup copy to transfer data to the administrator's workstation.

2. Shut down the operating system of the Administration Server.

3. Disconnect the network adapter from the corporate network.

4. Release the IP address of the device if you want to use it for the new installation of Kaspersky Security Center Linux.

5. Make sure the device is completely disconnected.

The presence of the old Administration Server is on the network may cause device management faults and interfere with the logon process in the Web Console of the new Administration Server; it can also make the Network Agent installation task connect to the old server.

## 3 Installing Kaspersky Security Center Linux using the quick installation script

These instructions describe the initial deployment of an instance of Kaspersky Security Center Linux using the quick installation script.

**Special considerations:**

- All components of Kaspersky Security Center are installed on the same device as the Administration Server.
- The operating system of the Administration Server is one of the following:
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.8.5) with PostgreSQL 15.
  - Ubuntu Server 26.04 LTS with PostgreSQL 18.
  - CentOS Stream 10 with PostgreSQL 18.
  - RED OS 8 with PostgreSQL 16.
- The quick installation script only automates the configuration and installation of the Kaspersky Security Center application. The administrator must take steps to configure the name of the Administration Server device in the operating system, the network adapters, security firewalls at the operating system level, and the hardware.

Initial installation of a Kaspersky Security Center Linux instance using the quick installation script involves the following steps:

**1. Preparation for deployment**

Before proceeding with the installation, prepare the following:

- The installation disk image of the operating system and the application package repository.
- An authenticator application for two-factor authentication (2FA) when logging in to the Web Console.
- New FQDN (for example, *ksclinux.example.com*). If you have sufficient experience in configuring the solutions, you can devise your own scenario for assigning the old FQDN to the new server during installation. In this case, at step 5 "Configuring the application after restoring from a backup copy", skip step 4. "Restoring the connection of managed devices to the FQDN of the previous Administration Server".
- The administrator's workstation with a browser for internet access to download distribution packages and manage the Web Console.
- Make sure the DNS server and the time server (NTP) are available for application components.
- Depending on the scenario, release the old IP address if an IP address was used for managed device connections.
- Configure network equipment and the proxy server in accordance with the requirements:
  - Ports for communication of application components.
  - Access to Kaspersky servers.
  - Hardening Guide.

**2. Sizing and operating system setup**

1. Configure the hardware depending on the number of devices that you want the Administration Server to manage.

A sizing calculation must take into account the resources available to Kaspersky applications. The sizing calculation allows for the Administration Server, Network Agent, DBMS, Web Console Server and Kaspersky Security Center Linux working together on the same device. The calculation does not cover the storage of backup copies of the Administration Server.

> Use an external file share as a mount point to store backup copies on a separate device; alternatively, provision extra free space on your hard disk to allow for backup storage.

We recommend adding an additional 4–6 GB of RAM and 20 GB of free hard disk space for the operating system.

Device sizing calculation depending on the managed device count:

- **S** (up to 1000 devices): 8 CPU cores, 16 GB of RAM, 70 GB of free hard disk space for the `/var` directory, 300 IOPS or more.
- **M** (up to 10,000 devices): 12 CPU cores, 24 GB of RAM, 340 GB of free hard disk space for the `/var` directory, 300 IOPS or more.
- **L** (up to 30,000 devices): 20 CPU cores, 40 GB of RAM, 490 GB of free hard disk space for the `/var` directory, 300 IOPS or more.
- **XL** (up to 50,000 devices): 28 CPU cores, 54 GB of RAM, 640 GB of free hard disk space for the `/var` directory, 300 IOPS or more.

2. Prepare the hardware for the Kaspersky Security Center Linux server in accordance with your sizing choices.

3. Install the operating system on the Kaspersky Security Center Linux server.

   During installation, enable the **SSH remote connection tools** option if you intend to manage the Administration Server device remotely on the command line.

   > Astra Linux must be installed without the **Mandatory Access Control** option. Also, for Kaspersky Endpoint Security for Linux to work correctly, you need to disable the **Prevent ptrace tracing** option.

4. Verify that you have enough free space for the `/var` directory if it is mounted separately, or for the root `/` directory.

   Examples for the M configuration:

   Astra Linux

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                 Size  Used Avail Use% Mounted on
   /dev/mapper/astra48242-01  406G  8,0G 377G    3% /
   <...>
   ```

   Ubuntu

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                         Size  Used Avail Use% Mounted on
   /dev/mapper/ubuntu--vg-ubuntu--lv  406G   11G  374G   3% /
   <...>
   ```

5. If the managed devices used an IP address for their connections, configure the IP address of the old Administration Server on the new server.

*Video: configuring the operating system*{[Start_Delete_en-US]}




{[End_Delete_en-US]}




### 3. Downloading the distribution files

1. Download the distribution packages of the required localization from the Kaspersky website and save these in a separate directory (for example, *kscdistr*).

   **For Ubuntu and Astra Linux**

   - Administration Server distribution package in deb format:
     `Version 16.3.0.1207 | Debian x64 | Administration server`
   - Web Console distribution package in deb format:
     `Version 16.3.0.1207 | Debian x64 | Web console`
   - Quick installation script:
     `Version 16.3.0.1207 | Linux | KSC installation script`

   **For CentOS and RED OS**

   - Administration Server distribution package in rpm format:
     `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Administration server`

- Web Console distribution package in rpm format:

  `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Web console`

- Quick installation script:

  `Version 16.3.0.1207 | Linux | KSC installation script`

2. For Kaspersky applications to work in Astra Linux's Closed software environment mode, download the kaspersky_astra_pub_key.gpg public key file.

3. Copy the downloaded files to the new Kaspersky Security Center Linux Administration Server device using removable media or over the network.

   The following paragraphs describe what you need to do on the command line to copy files over the network.

   > Whether you can use the scp utility to copy the data depends on the whether the SSH service is installed and running in the operating system of the Administration Server device and the security policy of your organization.

   a. On the command line, use the cd command to change to the directory one level above the *kscdistr* directory, for example:

   For Linux

   ```
   cd /home/administrator/Desktop
   ```

   For Windows

   ```
   cd C:\Users\Administrator\Downloads
   ```

   b. Copy the distribution files over the network using the scp utility:

   ```
   scp -r <kscdistr> <administrator>@<ksclinux.example.com>:
   ```

   where:

   `<kscdistr>` is the local directory with downloaded Kaspersky Security Center Linux distribution packages.

   `<administrator>` is the privileged user on the new Administration Server with SSH connection rights.

   `<ksclinux.example.com>` is the FQDN of the new Administration Server.

   The files are copied to the home directory of the user specified for the connection.

### 4. Configuring the installation

1. On the new Administration Server device, log in as a super user and start the command line.

2. Change to the directory with the copied distribution packages.

   Example

   ```
   cd ~/kscdistr
   ```

3. Extract the quick installation script from the archive into the current directory with distribution files.

Example

```
tar -xf ./ksc_fast_install.tar.gz
```

4. Make sure you have all files by running the following command:

```
ls -la
```

Example of ls -la output

```
administrator@ksclinux:~$ ls -la
drwxr-xr-x  3 administrator administrator      4096 jul 17 20:32 .
drwx------ 17 administrator administrator      4096 jul 17 17:54 ..
-rw-r--r--  1 administrator administrator       493 apr 20  2023 kaspersky_astra_pub_key.gpg
-rw-r--r--  1 administrator administrator 199128488 jul 10 21:38 ksc64_16.3.0-1207_amd64.deb
-rwxr-xr--  1 administrator administrator    143288 jul 22 17:22 ksc_fast_install.py
-rw-r--r--  1 administrator administrator 158144492 jul 10 21:37 ksc-web-console-16.3.12907.x86_64.deb
-rw-r--r--  1 administrator administrator     15561 jul 22 23:17 nwc_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 nwc_license.txt.sha256
-rw-r--r--  1 administrator administrator       493 jul 22 17:22 params.txt
-rw-r--r--  1 administrator administrator     70869 jul 22 23:17 server_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 server_license.txt.sha256
```

5. In the directory with distribution files, open the text file with the installation script parameters for editing, for example:

```
nano ./params.txt
```

6. Set the previously prepared values and uncomment the required lines (delete the `#` character at the beginning of the line), or add new lines with the following values:

   - Hardware sizing option (possible values: S/M/L/XL).

     Example

     ```
     klfi_netsize=S
     ```

   - FQDN of the Administration Server in two parameters of the file.

     ```
     klfi_klserver_address=ksclinux.example.com
     ```

     ```
     klfi_kliam_address=ksclinux.example.com
     ```

The language of the installed Administration Server depends on the localization of the downloaded distribution package.

7. Verify that the FQDN address of the Administration Server is being converted correctly to the loopback IP address in the operating system of the new Administration Server. To do this:

   a. Run the `ping` command with the address of the new Administration Server.

   Example of successfully getting a loopback IP address

   ```
   administrator@ksclinux:~$ ping ksclinux.example.com
   ping ksclinux.example.com
   PING ksclinux.example.com (127.0.1.1) 56(84) bytes of data.
   64 bytes from ksclinux.example.com (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
   ```

   b. Add the address of the Administration Server to the `/etc/hosts` file of the operating system of the new Administration Server if an address was not obtained or if an external IP address was obtained.

   To do this:

   - Open the `/etc/hosts` file for editing by running the following command:

     ```
     sudo nano /etc/hosts
     ```

   - Enter the address of the server as the FQDN of the Administration Server device, for example:

     ```
     127.0.0.1       localhost
     127.0.1.1       ksclinux.example.com ksclinux
     <...>
     ```

> On managed devices, the FQDN address of the Administration Server must be resolved to the external IP address of the server. Make sure the records on DNS servers are configured correctly.

**5. Running the quick installation script**

{[Start_Delete_en-US]}If using the closed software environment mode in Astra Linux:

- Use the maximum integrity level (High – level 63) for the user performing the installation in Astra Linux with the **Mandatory Integrity Control** mechanism enabled.
- Follow the additional steps:

  1. Change to the directory with the copied distribution packages, for example:

     ```
     cd ~/kscdistr
     ```

  2. Create a directory for the public key file under the system-wide configuration directory:

     ```
     sudo mkdir -p /etc/digsig/keys/legacy/kaspersky/
     ```

  3. Move the public key file `kaspersky_astra_pub_key.gpg` to the directory:

     ```
     sudo mv ./kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
     ```

4. Install the compatibility package:

```
sudo apt install -y astra-digsig-oldkeys
```

5. Update the system boot image:

```
sudo update-initramfs -u -k all
```

6. Restart the operating system:

```
sudo reboot
```

{[End_Delete_en-US]}

*To run the quick installation script:*

1. After restarting the device, go back to the directory with the distribution files:

```
cd ~/kscdistr
```

2. Make the quick installation script file executable by running the following command:

```
chmod +x ./ksc_fast_install.py
```

3. Read the terms and conditions of the End User License Agreement for your localization before you run the script because the quick installation script can display the legal information only in English.

4. Set up network package repositories for your operating system to be able to download packages during installation, or mount an operating system installation disk image.

5. Run the quick installation script:

```
sudo ./ksc_fast_install.py
```

6. Follow the steps of the setup wizard.

If at the step of determining the available resources, the script mistakenly finds insufficient RAM, disable dynamic RAM allocation for the duration of the installation.

7. Wait for the installation to finish. Review the text output of the script and save the username (`User`) and password (`Pass`) that you will use to log in to the Web Console.

Example

```
[+] Creating KSC user 'kscadmin' ...
[+] An internal user has been created:
[+]     User: kscadmin
[+]     Pass: ############
[!] If the password is lost, you must create a user by running the command:
        /opt/kaspersky/ksc64/sbin/kladduser -n <user>
[+] OK
[+] Success
```

{[Start_Delete_en-US]} *Video: Running the quick installation script for Astra Linux*




{[End_Delete_en-US]}

*Video: Running the quick installation script for Ubuntu*




**6. Logging in to the Web Console for the first time**

1. In your browser, open the address for connecting to the Web Console: `https://<FQDN>:8080`

   where `<FQDN>` is the Administration Server address from the script installation settings, for example, *https://ksclinux.example.com:8080*.

2. To log in to the Web Console, use the user name and password from the script output.

3. Configure the authenticator application:

    a. Copy the secret key for getting one-time codes to the application or scan the QR code from the Web Console authentication configuration wizard.

    b. Enter the generated code to authenticate and log in to the Web Console.

4. Review and confirm that you have read the Hardening Guide.

5. Configure the Administration Server in the quick start wizard if you do not intend to restore Administration Server data from a backup copy.

## 4 Restoring from a backup copy of Administration Server

If migrating from Kaspersky Security Center Windows or migrating data from Kaspersky Security Center Linux to new hardware, you may need to restore data from a backup copy made in the old installation of Administration Server.

> The PostgreSQL version of the new server must be at least the same as the version that the backup copy was made from.

Skip this step if you do not need to restore data.

If a backup copy has not been created in advance:

- Create a backup copy of the old Administration Server installation in the PostgreSQL data format.
- Install the new Kaspersky Security Center Linux server and log in to the Web Console for the first time.

Restoring from a backup copy of Administration Server involves the following steps:

**1. Transferring the backup copy to the Administration Server**

Transfer the backup copy of the old Administration Server to the new Administration Server device using removable media or over the network.

*To transfer the backup copy to the Administration Server over the network:*

> Whether you can use the scp utility to copy the data depends on the whether the SSH service is installed and running in the operating system of the Administration Server device and the security policy of your organization.

1. On the command line of the device, use the *cd* command to change to the directory containing the files of the backup copy of the old Administration Server, for example:

   Windows

   ```
   cd C:\kscbackups
   ```

   Linux

   ```
   cd /root/kscbackups
   ```

2. Copy the directory containing the files of the backup copy using the scp utility:

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   where:

   `<klbackup202x-xx-xx>` is the directory with the files of the backup copy.

   `<administrator>` is the privileged user on the new Administration Server with SSH connection rights.

   `<ksclinux.example.com>` is the FQDN of the new Administration Server.

   The directory with the backup copy is copied to specified user's home directory.

**2. Procedure for restoring from a backup copy**

1. On the new Administration Server device, open the command line.

2. While you are restoring data from a backup copy, temporarily grant PostgreSQL superuser rights to the standard klserver and kliam accounts that the Administration Server uses to connect to the DBMS:

   ```
   sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
   ```

   ```
   sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
   ```

3. Use the klbackup utility to start data restoration from the backup copy of the old Administration Server:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
   ```

   where `</home/administrator/klbackup202x-xx-xx>` is the full path to the directory containing the files of the backup copy.

4. If no password has been set for the backup copy, when prompted for the backup copy password, press **Enter** without entering a password.

5. Wait until the utility finishes.

   Large installations can take a long time.

6. Restore the original rights of the PostgreSQL accounts that the Administration Server uses to connect to the DBMS.

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

## 5 Configuring the application after restoring from a backup copy

Skip this step if you did not restore data from a backup copy.

The procedure for configuring the application after restoring from a backup copy involves the following steps:

### 1. Restoring the Web Console

1. Get the address of the old server from the IAM Server configuration file:

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Example

```
ksc_address: "oldksc.example.internal"
```

2. Verify that the FQDN address of the old Administration Server is being converted correctly to the loopback IP address of the new Administration Server. To do this:

   a. Run the `ping` command with the address of the old Administration Server.

Example of successfully getting a loopback IP address

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

   b. Add the address of the old Administration Server to the `[[/etc/hosts]]` file of the operating system of the new Administration Server, if the address was not obtained or if an external IP address was obtained. To do this:

   - Open /etc/hosts for editing:

```
sudo nano /etc/hosts
```

- Enter the name of the old server as an additional alias for the Administration Server device address.

  Example

  ```
  127.0.0.1       localhost
  127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
  <...>
  ```

3. Reinstall the Web Console.

   a. Delete the local Web Console Server:

   Depending on your Kaspersky Security Center Linux distribution, run one of the following commands:

   - For a device running a Debian-based operating system:

     ```
     sudo apt remove ksc-web-console -y
     ```

   - For a device running a Red Hat Enterprise Linux-based operating system:

     ```
     sudo dnf remove ksc-web-console -y
     ```

   b. Start the installation of the Web Console package from the directory with distribution packages:

   - On a device running a Debian-based operating system:

     ```
     sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
     ```

   - For a device running a Red Hat Enterprise Linux-based operating system:

     ```
     sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
     ```

**2. Restoring kscadmin user access for migration from Kaspersky Security Center Windows**

The user database has been overwritten; create the kscadmin user and configure two-factor authentication from scratch.

1. Open the command line in the operating system of the Administration Server device and run the following command to create a user:

   ```
   sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
   ```

   After pressing **Enter**, set a password, then re-enter the password.

2. In your browser, open the address for connecting to the Web Console:

   ```
   https://<FQDN>:8080
   ```

   where <FQDN> is the Administration Server address from the script installation settings, for example, *https://ksclinux.example.com:8080*.

3. Use the generated user name and password to log in to the Web Console.

4. Configure an authenticator application. To do this:

   a. Delete the old kscadmin user account profile that was configured in your authenticator application before you began restoring the backup copy of the Administration Server.

   b. Copy the secret key for getting one-time codes to the application or scan the QR code from the Web Console authentication configuration wizard.

   c. Enter the generated code to authenticate and log in to the Web Console.

**3. Testing the Administration Server**

1. Test the Web Console interface as the kscadmin user and other users.

2. Run the following tasks in sequence:

   - Download updates to the Administration Server repository
   - Administration Server maintenance
   - Backup of Administration Server data

   > Replace the Windows paths in the task settings with Linux paths of the new Administration Server, or delete the tasks and configure new tasks from scratch.

3. Review the results of the tasks and, if necessary, make changes to the settings of the tasks, management policies and Administration Server settings.

**4. Restoring the connection of managed devices to the FQDN of the previous Administration Server**

If you assigned a new FQDN address to the new Administration Server (for example, ksclinux.example.com), add one of the following types of DNS records:

- A CNAME record mapping the old Administration Server name to the new Administration Server name.

  For more information about configuring the required records, refer to your DNS server documentation.

- An A and AAAA record for the old Administration Server address pointing to the new Administration Server IP address.

  For a DNS service based on Windows Server, run commands with values that are applicable to your infrastructure.

*To add a DNS A record for a DNS service based on Windows Server, run the commands using values that are applicable to your infrastructure:*

1. Connect to the DNS server.

2. Open PowerShell and get the IP address from the existing A record by running the following command:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

3. Change the IP address in the A record by running the following commands:

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. Make sure the IP address in the A record has been updated by running the following command:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

The command output displays the IP address of the Kaspersky Security Center Linux Administration Server. Managed devices will restore their connections after updating the local DNS cache.

## 6 Configuring Anti-Virus protection of the Administration Server

To comply with the hardening guidelines in terms of providing the Administration Server with anti-virus protection, install Kaspersky applications on the Administration Server and configure management policies. To deploy Kaspersky Endpoint Security for Linux, follow its deployment guide.

Installation and configuration involves the following steps:

**1. Creating a separate administration group**

1. In the main window of the Web Console, select **Asset management** → **Hierarchy of groups**.
2. Select the check box next to the **Managed devices** group.
3. Click **Add**.
4. In the displayed window, enter a name for the new group (for example, *kscserver*) and confirm its creation by clicking the **Add** button.

**2. Creating a policy for the Network Agent without inheritance of settings**

1. In the main window of the Web Console, go to the **Asset management** → **Policies** section.
2. Then click the **Add** button.
3. In the New policy wizard, select the **Kaspersky Security Center Linux Network Agent** application and click **Next**.
4. Disable the **Inherit settings from parent policy** option and click **Save**.

### 3. Installing the Kaspersky Endpoint Security for Linux management plug-in from Kaspersky Security Center or manually

You can install the management plug-in for Kaspersky Endpoint Security for Linux in the following ways:

- From the list of available distribution packages in the Web Console
- Manually from a file

*To install the Kaspersky Endpoint Security management plug-in from the list of available distribution packages in the Web Console:*

1. In the main window of the Web Console, select **Settings** → **Web plug-ins**.

   This opens the list of installed web plug-ins.

2. Then click the **Add** button.

   The list of available management plug-ins is displayed. This list is automatically updated whenever a new version of a web plug-in is released.

3. In the list of available plug-ins, select the latest available version of the Kaspersky Endpoint Security for Linux web plug-in.

4. In the displayed web plug-in description window, click the **Install plug-in** button.

5. Wait until the installation is complete and click the **OK** button in the information window.

The new plug-in is added to the list of installed web plug-ins.

*Video: installing the web plug-in using the wizard*




*To install the Kaspersky Endpoint Security management plug-in manually from a file:*

1. Download the archive with the web plug-in from the application download page in the Kaspersky Endpoint Security for Linux section: **Application Control plug-in** → **Web console Plug-In**.

2. Unpack the downloaded archive locally.

3. In the main window of the Web Console, select **Settings** → **Web plug-ins**.

   This opens the list of installed web plug-ins.

4. Click the **Add from file** button.

5. In the displayed window, enter the path to the plugin.zip file and the path to the signature.txt file.

   These files are located in the folder in which unpacked the archive with the web plug-in.

6. Then click the **Add** button.

7. Wait until the installation is complete and click the **OK** button in the information window.

The new plug-in appears in the list of installed web plug-ins (**Settings** → **Web plug-ins**).

*Video: installing the management web plug-in in isolated networks*




**4. Creating a policy for Kaspersky Endpoint Security for Linux without inheritance of settings**

When using Kaspersky Endpoint Security for Linux together with Kaspersky Security Center Linux, you need to configure the policy in accordance with the recommendations of Kaspersky experts.

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Select an administration group for the Administration Server.

3. Click **Add**.

   The New policy wizard starts.

4. In the displayed window, select the Kaspersky Endpoint Security for Linux application from the list.

5. Specify the **Standard mode or the Kaspersky Endpoint Detection and Response Agent mode** for Kaspersky Endpoint Security for Linux.

6. Make a decision about using Kaspersky Security Network.

7. Review the optimization guidelines for managed devices.

8. In the name of the policy, indicate that the policy belongs to the Administration Server.

9. Disable the **Inherit settings from parent policy** option.

10. Save your changes.

*Video: creating a policy*




**5. Creating an Update group task for Kaspersky Endpoint Security for Linux**

1. In the main window of the Web Console, select the **Tasks** section.

2. Select an administration group for the Administration Server.

3. Click **Add**.

   The New task wizard starts.

4. In the displayed window, select the Kaspersky Endpoint Security for Linux application from the list.

5. Specify the *Update* task type and click through the next steps without changing any settings.

   This opens the task properties window.

6. In the **Application settings** → **Sources of updates** section, enable the Kaspersky Security Center source and raise its priority.

In an isolated network, use the Kaspersky Update Utility to create a repository for update tasks.

*Video: configuring centralized database updates*




**6. Adding a license key to the Administration Server repository with automatic distribution**

1. In the main window of Kaspersky Security Center Web Console, select the **Licenses** section.
2. Click **Add**.
3. Select the **Activation code** option and click **Send**.

   In an isolated network, use a key file that you can request using the service at https://keyfile.kaspersky.com/en.
4. In the list of licenses, click the name of the license.
5. Select the **Automatically distribute license key to managed devices** check box.
6. Save your changes.

*Video: activating the application with an activation code*



*Video: activating the application with a key file*




**7. Creating installation packages for the Network Agent and Kaspersky Endpoint Security for Linux**

1. In the main window of the Web Console, select **Software management** → **Installation packages**.
2. Click **Add**.

   The New package wizard starts.
3. Select **Create an installation package for a Kaspersky application**.
4. In the list of applications, find the latest version of Kaspersky Endpoint Security for Linux and click its name.
5. In the sidebar, start the download by clicking the **Download and create installation package** button.

   Review and accept the license agreements to start using the applications.
6. Return to the list of applications and download the latest version of the Kaspersky Network Agent for Linux.

   Review and accept the license agreements to start using the applications.
7. In the main window of the Web Console, in the list of downloaded applications, click the names of the applications.

In an isolated network, download the distribution packages from the Kaspersky website and in the New package wizard, select the **Create an installation package from a file** option.

*Video: automatic creation of an installation package in Kaspersky Security Center*




*Video: manual creation of an installation package from a file in Kaspersky Security Center*




**8. Installing Network Agent for Linux**

1. In the main window of the Web Console, select **Software Management** → **Installation packages**.
2. Select the check box next to the **Kaspersky Network Agent for Linux** package.
3. Click **Deploy**.

   The Protection deployment wizard starts.
4. Select the **Using a stand-alone package** option.
5. At the **Move devices to the Managed devices folder** step, skip configuring the rules for moving devices to an administration group. This option is not applicable to the Administration Server device.
6. At the **Result of stand-alone installation package creation** step, select and copy the full path to the application installation script.
7. Open the command line of the operating system of the Administration Server.

8. Start the installation of the stand-alone package:

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

where `</var/opt/.../stand-alone_package_sh>` is the previously copied full path to the script file of the stand-alone installation package.

If the installation is successful, a notification is displayed to that effect.

9. Move the Administration Server device (for example, *ksclinux*) from the **Managed devices** group to the previously prepared administration group (for example, *kscserver*).

**9. Installing Kaspersky Endpoint Security for Linux**

1. In the main window of the Web Console, select **Software Management** → **Installation packages**.
2. Select the check box for the Kaspersky Endpoint Security for Linux package.
3. Click **Deploy**.

   The Protection deployment wizard starts.
4. Select the **Using a stand-alone package** option.
5. At the **Result of stand-alone installation package creation** step, select and copy the full path to the application installation script.
6. Open the command line of the operating system of the Administration Server.
7. Start the installation of the stand-alone package:

```
sudo bash "</var/opt/.../stand-alone_package_sh>"
```

where `</var/opt/.../stand-alone_package_sh>` is the previously copied full path to the script file of the stand-alone installation package.

If the installation is successful, a notification is displayed to that effect.

8. In the main window of the Web Console, in the **Tasks** section, select the root node in the list of administration groups with the name of the Administration Server.
9. From the list of Administration Server tasks, start the following tasks in sequence:
   - "Download updates to the Administration Server repository"
   - Update (Kaspersky Endpoint Security for Linux)
10. In the main window of the Web Console, select **Asset management** → **Managed devices**.
11. Click the name of the Administration Server device object.
12. Review the values of the main indicators of the device status:
    - Anti-virus databases last updated (up-to-date)
    - Connected to Administration Server (up-to-date)

- Protection status (Running)
- *Key added successfully* event (present)

Follow the Kaspersky Endpoint Security for Linux deployment guide to deploy the application to devices on your network.

# Migration to Kaspersky Security Center by using the Migration wizard

Following this scenario, you can transfer the administration group structure, included managed devices and other group objects (policies, tasks, global tasks, tags, and device selections) from Kaspersky Security Center Windows under management of Kaspersky Security Center Linux.

Data migration to Kaspersky Security Center is possible with Kaspersky Security Center Windows version 15.1.0.22239 or later.

**Features of the migration method**

- Partial migration of Administration Server data
- Selection of objects for migration is available
- Administration group or subgroup to be migrated can contain no more than 10,000 devices
- Used to partially transfer Administration Server data, including only group objects within the migration scope; group objects outside the migration scope must be restored manually

**Migration scope**

- Structure of administration groups
- Managed devices included in administration groups (no more than 10,000 devices)
- Tags assigned to migrating devices
- Global tasks of Network Agent and managed applications (not for Administration Server)
- Group tasks of Network Agent and managed applications
- Policies of managed applications
- Report templates
- User role
- Internal users and security groups
- Custom application categories with content added manually
- Custom device selections

**Limitations**

- Migration is only possible from Kaspersky Security Center Windows version 15.1 or later to Kaspersky Security Center Linux version 15 or later.
- You can perform this scenario only by using Kaspersky Security Center Web Console.
- The following scopes cannot be migrated:
  - Global tasks of Administration Server
  - Events saved on the Administration Server
  - Repository of distribution packages of applications for remote installation
  - Administration Server certificate
  - License keys used by Administration Server and managed applications
  - Virtual Administration Servers
  - Network Agent policy settings
  - Device moving rules
  - Rules for auto-tagging devices
  - Distribution points
  - Kaspersky application settings saved on the Administration Server

Before you begin, learn more about the features and limitations of Kaspersky Security Center Linux:

- Functional differences between Kaspersky Security Center Windows and Kaspersky Security Center Linux
- List of Kaspersky applications supported by Kaspersky Security Center Linux

## Stages

The migration scenario proceeds in stages:

### 1 Preliminary steps

This step contains instructions for preparing a previously configured Administration Server to subsequent migration to the new Kaspersky Security Center Linux Administration Server. The preliminary steps are as follows:

1. Check the version of the Administration Server to create a backup copy compatible with Kaspersky Security Center Linux.

All current versions of **Kaspersky Security Center Linux** support data migration when upgrading to a newer version of the application. Backup copies can be created and restored only within one type of DBMS.

For **Kaspersky Security Center Windows**, check the version of the Administration Server in **Properties** → **General** → **Version**. If the version is earlier than 15.1.0.22239, upgrade Kaspersky Security Center Windows to the latest version.

**Upgrading Kaspersky Security Center Windows to the latest version**

1. From the Kaspersky website, download the distribution package corresponding to the localization language of your installed Administration Server: `Version 15.1.0.22239 | Windows | Full distributive`.

   The executable file is saved to your **Downloads** folder with the following name: `ksc_15.1_<build number>_full_<language>.exe`.

2. Copy the distribution package to the Administration Server.

3. Run the `ksc_15.1_<build number>_full_<language>.exe` executable file as administrator.

4. In the displayed window, click the **Install Kaspersky Security Center** link.

   The Administration Server Setup wizard starts.

5. Read the License Agreement and Privacy Policy. If you agree with all the terms and conditions of the End User License Agreement and the Privacy Policy, select the following check boxes under **I confirm that I have fully read, understand, and accept the terms and conditions of the following**:

   - **The terms and conditions of this EULA**.
   - **Privacy Policy describing the handling of data**.

6. Select **Upgrade Administration Server and web-based console (recommended)** and go to the next step.

7. Create a new backup copy by selecting **I want to create a backup copy of data** and completing the backup wizard.

8. Click **Upgrade**.

9. During the upgrade, in the Web Console setup wizard, confirm all steps of the wizard to upgrade the version.

   The upgrade process takes some time. After the setup wizard has finished, the Administration Console may not accept connections until the database is initialized.

10. Wait until the upgrade is complete.

2. Check the Administration Server certificate for compliance.

   Before creating a backup copy, make sure that the certificate contains the Subject Alternative Name (SAN). If not, it is important to replace the certificate, otherwise you will not be able to log in to the Web Console after restoring from a backup copy.

*To verify that the certificate includes a Subject Alternative Name:*

- For a Windows-based device:

  a. In the Administration Console, select the Administration Server that you want to check.

  b. In the context menu, select **Properties** → **General** → **View Administration Server certificate**.

  c. In the displayed window, check the **Subject Alternative Name** value.

- For a Linux device, run the following command:

```
sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
```

Make sure that the Subject Alternative Name contains the domain name (DNS) of the Administration Server host.

If the value contains only an external IP address without a domain name (DNS), or the value is missing altogether, manually replace the certificate with a certificate that meets the requirements for working with Kaspersky Security Center Linux. Replace the Administration Server general certificate by using the klsetsrvcert utility.

**Replacing the Administration Server general certificate by using the klsetsrvcert utility**

1. Create a new certificate with a delayed start date of use on devices by running the following command:

   - For Kaspersky Security Center Windows:

```
"%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
<oldksc.example.internal>" -o "RsaKeyLen:2048"
```

   - For Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
```

   where `"<oldksc.example.internal>"` is the FQDN of the connection to the Administration Server.

   Do not use an IP address for this value.

2. Set the start date for the new certificate on all hosts by running the following command:

   - For Kaspersky Security Center Windows:

```
"%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
```

   - For Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
```

   where the `"DD-MM-YYYY hh:mm"` date is at least 30 days after the current date. By default, the distribution period for a new certificate (`CR`) is 90 days.

When the configured time comes, you will need to reinstall the Web Console to restore access to it and have its certificate actualized.

3. If necessary, after migration to a new Administration Server, run the klmover utility to restore the connection of hosts to the Administration Server. You may need to run the utility if the host has been powered off for the entire certificate distribution period or if it has not connected to the Administration Server.

## 2 Choose a migration method

You migrate to Kaspersky Security Center Linux through the Migration wizard. The Migration wizard steps depend on whether or not Administration Servers of Kaspersky Security Center Windows and Kaspersky Security Center Linux are arranged into a hierarchy:

- Migration by using a hierarchy of Administration Servers

  Choose this option if Administration Server of Kaspersky Security Center Windows acts as secondary to Administration Server of Kaspersky Security Center Linux. You manage the migration process and switch between Servers within a single instance of Kaspersky Security Center Web Console. If you prefer this option, you can arrange Administration Servers into a hierarchy to simplify the migration procedure. To do this, create the hierarchy before starting the migration.

- Migration by using an export file (ZIP archive)

  Choose this option if Administration Servers of Kaspersky Security Center Windows and Kaspersky Security Center Linux are not arranged into a hierarchy. You manage the migration process with two instances of Kaspersky Security Center Web Console—an instance for Kaspersky Security Center Windows and another one for Kaspersky Security Center Linux. In this case, you will use the export file that you created and downloaded during the export from Kaspersky Security Center Windows and import this file to Kaspersky Security Center Linux.

## 3 Back up the certificate and private key of Kaspersky Security Center Windows Administration Server (optional step)

You might want to put the managed devices under the management of the Administration Server of Kaspersky Security Center Linux through restoring the certificate and private key of Administration Server from a backup copy. In this case, back up the certificate and private key of Kaspersky Security Center Windows Administration Server. Then at stage 7 you have to restore the certificate and private key.

## 4 Export data from Kaspersky Security Center Windows

Open Kaspersky Security Center Windows, and then run the Migration wizard.

### 5 Import data to Kaspersky Security Center Linux

Continue the Migration wizard to import the exported data to Kaspersky Security Center Linux. If the Servers are arranged into a hierarchy, the import starts automatically after a successful export within the same wizard. If the Servers are not arranged into a hierarchy, you continue the Migration wizard after switching to Kaspersky Security Center Linux.

### 6 Perform additional actions to transfer objects and settings from Kaspersky Security Center Windows to Kaspersky Security Center Linux manually (optional step)

You might also want to transfer the objects and settings that cannot be transferred through the Migration wizard. For example, you could additionally do the following:

- Transfer the license keys used by Administration Server and managed applications
- Configure global tasks of Administration Server
- Configure Network Agent policy settings
- Create installation packages of applications
- Create virtual Servers
- Configure device moving rules
- Configure rules for auto-tagging devices
- Create application categories
- Assign and configure distribution points

  If you move a device that acts as a distribution point to another Administration Server, the devices included in the scope of the distribution point are not moved automatically. You have to move each device individually. If a distribution point is acting as a gateway, you have to run the `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl` script so that the distribution point no longer serves as a gateway.

### 7 Move the imported managed devices under management of Kaspersky Security Center Linux

To complete the migration, move the imported managed devices under management of Kaspersky Security Center Linux. You can do it by one of the following methods:

- Through the klmover utility

  Use the klmover utility and specify the connection settings for the new Administration Server.

- Through the *Change Administration Server* task

  Create a *Change Administration Server* task, specify the imported managed devices, new Administration Server, and other task settings. Then run the task to put the managed devices under the management of the Administration Server of Kaspersky Security Center Linux.

- Through removal (if already installed) and further installation of Network Agent on the managed devices

  Create a new Network Agent installation package and specify the connection settings for the new Administration Server in the installation package properties. Remove Network Agent on the imported managed devices, and then use the installation package to install Network Agent on the imported managed devices through a remote installation task. You can also create and use a stand-alone installation package to install Network Agent locally. For more information, see Switching managed devices under management of Kaspersky Security Center Linux.

- Through restoring the certificate and private key of Administration Server from a backup copy (only for migration to Kaspersky Security Center Linux version 15.1 or later)

  Assign the same network address to the device with Administration Server of Kaspersky Security Center Linux as on Administration Server of Kaspersky Security Center Windows. Run the klbackup utility with the `-cert_only` parameter to restore the Administration Server certificate and private key from the backup copy that you saved at stage 3. In the command line, execute the following command: `/opt/kaspersky/ksc64/sbin/klbackup -path <path to the backup copy of Administration Server certificate> -restore -cert_only`.

### 8 Update Network Agent to the latest version

Upgrade the Network Agent for Linux to the same version as Kaspersky Security Center.

### 9 Make sure the managed devices are visible on the new Administration Server

On Kaspersky Security Center Linux Administration Server, open the managed devices list (**Asset management** → **Managed devices**), and check the values in the **Visible**, **Network Agent is installed**, and **Last connected to Administration Server** columns.

## Other methods of data migration

Besides the Migration wizard, there are other methods to transfer your current objects, but these methods allow you to transfer only policies and tasks:

- Export the tasks from Kaspersky Security Center Windows, and then import the tasks to Kaspersky Security Center Linux.

- Export specific policies from Kaspersky Security Center Windows, and then import the policies to Kaspersky Security Center Linux. The related policy profiles are exported and imported together with the selected policies.

# Exporting group objects from Kaspersky Security Center Windows

Migration administration group structure, included managed devices and other group objects from Kaspersky Security Center Windows to Kaspersky Security Center Linux requires that you first select data for exporting and create an export file. The export file contains information about all group objects that you want to migrate. The export file will be used for subsequent import to Kaspersky Security Center Linux.

You can export the following objects:

- Tasks and policies of managed applications
- Global tasks
- Custom device selections
- Administration group structure and included devices
- Tags that have been assigned to migrating devices

Before you start exporting, read general information about migration to Kaspersky Security Center Linux. Choose the migration method—by using or not using the hierarchy of Administration Servers of Kaspersky Security Center Windows and Kaspersky Security Center Linux.

*To export managed devices and related group objects through the Migration wizard:*

1. Depending on whether or not the Administration Servers of Kaspersky Security Center Windows and Kaspersky Security Center Linux are arranged into a hierarchy, do one of the following:
   - If the Servers are arranged into a hierarchy, open Kaspersky Security Center Web Console, and then switch to the Server of Kaspersky Security Center Windows.
   - If the Servers are not arranged into a hierarchy, open Kaspersky Security Center Web Console connected to Kaspersky Security Center Windows.
2. In the main menu, go to **Operations** → **Migration**.
3. Select **Migrate to Kaspersky Security Center Linux or Open Single Management Platform** to start the wizard and follow its steps.
4. Select the administration group or subgroup to export. Please make sure that the selected administration group or subgroup contains no more than 10,000 devices.
5. Select the managed applications whose tasks and policies will be exported. Select only applications that are supported by Kaspersky Security Center Linux. The objects of unsupported applications will still be exported, but they will not be operable.
6. Use the links on the left to select the global tasks, device selections, and reports to export. The **Group objects** link allows you to exclude custom roles, internal users and security groups, and custom application categories from the export.

The export file (ZIP archive) is created. Depending on whether or not you perform migration with Administration Server hierarchy support, the export file is saved as follows:

- If the Servers are arranged into a hierarchy, the export file is saved to the temporary folder on Kaspersky Security Center Web Console Server.
- If the Servers are not arranged into a hierarchy, the export file is downloaded to your device.

For migration with Administration Server hierarchy support, the import starts automatically after a successful export. For migration without Administration Server hierarchy support, you can import the saved export file to Kaspersky Security Center Linux manually.

# Importing the export file to Kaspersky Security Center Linux

To transfer information about managed devices, objects, and their settings that you exported from Kaspersky Security Center Windows, you must import it to Kaspersky Security Center Linux or Kaspersky Next XDR Expert.

*To import managed devices and related group objects through the Migration wizard:*

1. Depending on whether or not the Administration Servers of Kaspersky Security Center Windows and Kaspersky Security Center Linux are arranged into a hierarchy, do one of the following:
   - If the Servers are arranged into a hierarchy, proceed to the next step of the Migration wizard after the export is completed. The import starts automatically after a successful export within this wizard (see step 2 of this instruction).
   - If the Servers are not arranged into a hierarchy:
     a. Open the Kaspersky Security Center Web Console application connected to Kaspersky Security Center Linux or Kaspersky Next XDR Expert.
     b. In the main menu, go to **Operations** → **Migration**.
     c. Select the export file (ZIP archive) that you created and downloaded during the export from Kaspersky Security Center Windows. The upload of the export file starts.
2. After the export file is uploaded successfully, you can continue importing. If you want to specify another export file, click the **Change** link, and then select the required file.
3. The entire hierarchy of administration groups of Kaspersky Security Center Linux is displayed.

   Select the check box next to the target administration group to which the objects of the exported administration group (managed devices, policies, tasks, and other group objects) must be restored.
4. The import of group objects starts. You cannot minimize the Migration wizard and perform any concurrent operations during the import. Wait until the refresh icons (↻) next to all items in the list of objects are replaced with green check marks (✓) and the import finishes.
5. When the import completes, the exported structure of administration groups, including device details, appears under the target administration group that you selected. If the name of the object that you restore is identical to the name of an existing object, the restored object has an incremental suffix added.

If in a migrated task the details of the account under which the task is run are specified, you have to open the task and enter the password again after the import is completed.

If the import has completed with an error, you can do one of the following:

- For migration with Administration Server hierarchy support, you can start to import the export file again.
- For migration without Administration Server hierarchy support, you can start the Migration wizard to select another export file, and then import it again.

You can check whether the group objects included in the export scope have been successfully imported to Kaspersky Security Center Linux. To do this, go to the **Asset management** section and ensure whether the imported objects appear in the corresponding subsections.

Note that the imported managed devices are displayed in the **Managed devices** subsection, but they are invisible in the network and Network Agent is not installed and running on them (the *No* value in the **Visible**, **Network Agent is installed**, and **Network Agent is running** columns).

To complete the migration, you need to switch the managed devices to be under management of Kaspersky Security Center Linux.

# Switching managed devices to be under management of Kaspersky Security Center Linux

After a successful import of information about managed devices, objects, and their settings to Kaspersky Security Center Linux, you need to switch the managed devices to be under management of Kaspersky Security Center Linux to complete the migration.

You can move the managed devices to be under Kaspersky Security Center Linux by one of the following methods:

- Using the klmover utility.
- Using the *Change Administration Server* task.
- Restoring the certificate and private key of Administration Server from a backup copy (only for migration to Kaspersky Security Center Linux 15.1 or later).

  For details, see the "Move the imported managed devices under management of Kaspersky Security Center Linux" step in the main data migration scenario.
- Installing Network Agent on the managed devices through a remote installation task.

*To switch managed devices to be under management of Kaspersky Security Center Linux by installing Network Agent:*

1. Remove Network Agent on the imported managed devices that will be switched under management of Kaspersky Security Center Linux.
2. Switch to Administration Server of Kaspersky Security Center Windows.
3. Go to **Software management** → **Installation packages**, and then open the properties of an existing installation package of Network Agent.

If the installation package of Network Agent is absent in the package list, download a new one.

You can also create and use a stand-alone installation package to install Network Agent locally.

4. On the **Settings** tab, select the **Connection** section. Specify the connection settings of Administration Server of Kaspersky Security Center Linux.

5. Create a remote installation task for imported managed devices, and then specify the reconfigured Network Agent installation package.

   You can install Network Agent through Administration Server of Kaspersky Security Center Windows or through a Windows-based device that acts as a distribution point. If you use Administration Server, enable the **Using operating system resources through Administration Server** option. If you use a distribution point, enable the **Using operating system resources through distribution points** option.

6. Run the remote installation task.

After the remote installation task finishes successfully, go to Administration Server of Kaspersky Security Center Linux and ensure that managed devices are visible in the network, and that Network Agent is installed and running on them (the *Yes* value in the **Visible**, **Network Agent is installed**, and **Network Agent is running** columns).

# Configuring Administration Server

This section describes the configuration process and properties of Administration Server.

# Configuring the Administration Server connection address

The Administration Server connection address is the network address used for the following purposes:

- As a default address when creating the Network Agent installation packages

  After the installation of the Network Agent, managed devices connect to the Administration Server at this address.

- As the KSN proxy server address

  Managed devices connect to the KSN proxy server via this address.

*To configure the Administration Server connection address:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **General** section.

3. In the window that opens, in the **Administration Server connection address** field, specify the new Administration Server connection address.

   The maximum length of the connection address is 255 characters.

   You can specify the Administration Server connection address as the NetBIOS name, FQDN, or the IP address of the Administration Server.

4. Click the **Save** button.

The specified address is used as the Administration Server address and the KSN proxy server address.

# Configuring the connection of Kaspersky Security Center Web Console to Administration Server

You can configure the connection of Kaspersky Security Center Web Console to Administration Server through the Administration Server properties or by using the Administration Server policy settings.

*To set the connection ports through the Administration Server properties:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Connection ports** section.
3. If necessary, specify the **SSL port for Web Console** setting or specify other Administration Server connection ports.

The main connection settings of the selected Server are specified.

*To set the connection ports through the Administration Server policy settings:*

1. In the main menu, go to **Asset management** → **Policies**.
2. Click the name of the Administration Server policy, and then go to the **Application settings** tab.
3. If necessary, specify the **SSL port for Web Console** setting or specify other Administration Server connection ports.

> If you disable the **Open port for Web Console** option and this policy setting will be applied to the device, you will not be able to connect to the Administration Server by using Kaspersky Security Center Web Console. In this case, the connection will be terminated. If you have an Administration Server on which this policy is not applied, you can reconnect to this Administration Server through Kaspersky Security Center Web Console.

The main connection settings of the selected Server are specified.

# Configuring an allowlist of IP addresses to connect to Kaspersky Security Center Linux

By default, the connections to Kaspersky Security Center Linux are allowed from any device. For example, you can install Kaspersky Security Center Web Console Server on any device that meets the requirements, and Kaspersky Security Center Web Console Server will communicate with Kaspersky Security Center Linux. However, you can configure Administration Server so that the connections are only allowed from devices with the IP addresses that you specify. In this case, if an intruder tries to connect to Kaspersky Security Center Linux through Kaspersky Security Center Web Console Server installed on a device that is not included in the allowlist, he or she will not be able to log in to Kaspersky Security Center Linux.

The IP address is verified when a user logs in to Kaspersky Security Center Linux or runs an application that interacts with Administration Server via Kaspersky Security Center Linux OpenAPI. At this moment, an application on a device tries to establish a connection with Administration Server. If the IP address of the device is not in the allowlist, an authentication error occurs and the KLAUD_EV_SERVERCONNECT event notifies you that a connection with Administration Server has not been established.

## Requirements for an allowlist of IP addresses

IP addresses are verified only when the following applications try to connect to Administration Server:

- Kaspersky Security Center Web Console Server

  If you sign in to Kaspersky Security Center Linux through Kaspersky Security Center Web Console, you can configure a firewall on the device where Kaspersky Security Center Web Console Server is installed using the standard means of operating system. Then, if someone tries to log in to Kaspersky Security Center Linux on one device and Kaspersky Security Center Web Console Server is installed on another device, a firewall helps prevent intruders from interfering.

- Applications interacting with Administration Server via klakaut automation objects

- Applications interacting with Administration Server via OpenAPI, such as Kaspersky Anti Targeted Attack Platform or Kaspersky Security for Virtualization

Therefore, specify addresses of the devices on which the applications listed above are installed.

You can set IPv4 and IPv6 addresses. You cannot specify ranges of IP addresses.

## How to establish an allowlist of IP addresses

If you have not set an allowlist earlier, follow the instructions below.

*To establish an allowlist of IP addresses to log in to Kaspersky Security Center Linux:*

1. On the Administration Server device, run the command prompt under an account with administrator rights.
2. Change your current directory to the Kaspersky Security Center Linux installation folder (usually, /opt/kaspersky/ksc64/sbin).
3. Enter the following command under the root account:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP addresses>" -t s`

   Specify IP addresses that meet the requirements listed above. Several IP addresses must be separated by a semicolon.

   Example of how to allow only one device to connect to Administration Server:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Example of how to allow multiple devices to connect to Administration Server:

   `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. Restart the Administration Server service.

You can find out whether you have successfully configured the allowlist of IP addresses in the Syslog Event Log on the Administration Server.

### How to change an allowlist of IP addresses

You can change an allowlist just as you did when you first established it. For this purpose, run the same command and specify a new allowlist:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP
addresses>" -t s
```

If you want to delete some IP addresses from the allowlist, rewrite it. For example, your allowlist includes the following IP addresses: 192.0.2.0; 198.51.100.0; 203.0.113.0. You want to delete the 198.51.100.0 IP address. To do this, enter the following command at the command prompt:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0;
203.0.113.0" -t s
```

Do not forget to restart the Administration Server service.

### How to reset a configured allowlist of IP addresses

*To reset an already configured allowlist of IP addresses:*

1. Enter the following command at the command prompt under the root account:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Restart the Administration Server service.

After that, IP addresses are not verified any more.

# Configuring internet access settings for Administration Server

You must configure internet access to use Kaspersky Security Network and to download updates of anti-virus databases for Kaspersky Security Center Linux and managed Kaspersky applications.

*To specify the internet access settings for Administration Server:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Configuring internet access** section.

3. Enable the **Use proxy server** option if you want to use a proxy server when connecting to the internet. If this option is enabled, the fields are available for entering settings. Specify the following settings for a proxy server connection:

   **Proxy server address**

   Address of the proxy server used for Kaspersky Security Center Linux connection to the internet.

**Port number**

Number of the port through which Kaspersky Security Center Linux proxy connection will be established.

**Bypass proxy server for local addresses**

No proxy server will be used to connect to devices in the local network.

**Proxy server authentication**

If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

This entry field is available if the **Use proxy server** check box is selected.

**User name**

User account under which connection to the proxy server is established (this field is available if the **Proxy server authentication** check box is selected).

**Password**

Password set by the user under whose account the proxy server connection is established (this field is available if the **Proxy server authentication** check box is selected).

To see the entered password, click and hold the **Show** button for as long as you require.

You can also configure internet access by using the quick start wizard.

# Hierarchy of Administration Servers

Some client companies, for example MSP, may run multiple Administration Servers. It can be inconvenient to administer several separate Administration Servers, so a hierarchy can be applied. In a hierarchy, a Linux-based Administration Server can work both as a primary Server and as a secondary Server. The primary Linux-based Server can manage both Linux-based and Windows-based secondary Servers. A primary Windows-based Server can manage a secondary Linux-based Server.

A "primary/secondary" configuration for two Administration Servers provides the following options:

- A secondary Administration Server inherits policies, tasks, user roles, and installation packages from the primary Administration Server, thus preventing duplication of settings.
- Selections of devices on the primary Administration Server can include devices from secondary Administration Servers.
- Reports on the primary Administration Server can contain data (including detailed information) from secondary Administration Servers.
- A primary Administration Server can be used as a source of updates for a secondary Administration Server.

The primary Administration Server only receives data from non-virtual secondary Administration Servers within the scope of the options listed above. This limitation does not apply to virtual Administration Servers, which share the database with their primary Administration Server.

Hierarchy of Administration Servers provides support for multitenancy mode. This mode allows a main administrator to centrally manage multiple clients independently. Each client organization or office is isolated from others and is referred to as a tenant. You can allocate multiple managed devices along with their associated data, settings, policies, and tasks to a tenant, and configure user rights by tenant.

A primary Administration Server, installed in the main organization infrastructure, acts as a primary tenant. The primary Administration Server enables secondary or virtual Administration Servers—its isolated tenants—to independently receive and process their own events and work with their own resources, services, and configurations.

A service provider that has a number of client organizations can provide the Kaspersky Security Center Linux functionality, including alert aggregation and response actions, to each client organization independently. To achieve this, the service provider connects secondary or virtual Administration Servers as tenants for each client organization. The service provider delivers services by using their own personnel and resources.

# Creating a hierarchy of Administration Servers: adding a secondary Administration Server

In a hierarchy, a Linux-based Administration Server can work both as a primary Server and as a secondary Server. The primary Linux-based Server can manage both Linux-based and Windows-based secondary Servers. A primary Windows-based Server can manage a secondary Linux-based Server.

## Adding secondary Administration Server (performed on the future primary Administration Server)

You can add an Administration Server as a secondary Administration Server, thus establishing a "primary/secondary" hierarchy.

*To add a secondary Administration Server that is available for connection through Kaspersky Security Center Web Console:*

1. Make sure that port 13000 of the future primary Administration Server is available.

   This port will be used for interaction between primary and secondary Administration Servers after you build the hierarchy.

2. Go to the properties of the future primary Administration Server:

   a. In the main menu, select a section (except for **Marketplace**, **Console navigation**, and **Settings**), and then at the top of the page, click the **Show hierarchy** button.

   b. In the navigation pane that opens, hover the mouse cursor over the name of the required Administration Server, and then click the settings icon (⚙).

      Alternately, you can click the Administration Server name, and then, after the name is displayed in the main menu, click it in the main menu to open the server properties window.

3. In the properties window that opens, click the **Administration Servers** tab.

4. Select the check box next to the name of the administration group to which you want to add the Administration Server.

5. In the menu line, click **Connect secondary Administration Server**.

   The Add secondary Administration Server wizard starts. Proceed through the Wizard by using the **NEXT** button.

6. Fill in the following fields:

**Connect primary Administration Server to secondary Administration Server in DMZ**

Select this option if the secondary Administration Server is in a demilitarized zone (DMZ).

If this option is selected, the primary Administration Server initiates connection to the secondary Administration Server. Otherwise, the secondary Administration Server initiates connection to the primary Administration Server.

**Secondary Server display name**

A name by which the secondary Administration Server will be displayed in the hierarchy. If you want, you can enter the IP address as a name, or you can use a name like, for example, "Secondary Server for group 1".

**Secondary Server address**

Specify the IP address or the domain name of the secondary Administration Server.

This parameter is required if the **Connect primary Administration Server to secondary Administration Server in DMZ** option is enabled.

**Server SSL port**

Specify the number of the SSL port to be used for interaction between primary and secondary Administration Servers after you build the hierarchy. The default port number is 13000.

**Server API port**

The number of the port that Web Console will use for receiving connections from the secondary Administration Server over OpenAPI. The default port number is 13299.

While building the hierarchy, Web Console connects to the future secondary Server, requests credentials, retrieves the public certificate, and performs the initial setup.

After the hierarchy of Administration Server is built, port 13299 will no longer be used. Administration Servers will interact over port 13000.

**Certificate for secondary Administration Server**

Add a certificate file. You can either manually upload the certificate from you device or get it from the secondary Administration Server.

7. Specify the connection and authentication settings:

   - Enter the address of the future primary Administration Server.
   - Select the **Use proxy server** option if you use a proxy server to connect to the secondary Administration Server.

     In this case, you also have to specify the following settings of the proxy server:

     - **Proxy server address**
     - **User name**
     - **Password**

8. Enter the credentials of the user that has access rights on the future secondary Administration Server.

The wizard is finished, the connection with the future secondary Server is established, and the "primary/secondary" hierarchy is built.

Connection between the primary and secondary Administration Servers is established through port 13000. The tasks and policies from the primary Administration Server are received and applied. The secondary Administration Server is displayed on the primary Administration Server, in the administration group where it was added.

The connection fails in the following cases:

- The connection settings are incorrect.

  You have to check the settings or specify the certificate of the future secondary Server manually.

- The future secondary Server is authenticated with a self-signed certificate that was automatically generated by Kaspersky Security Center Linux. As a result, the browser might block downloading the self-signed certificate.

  You can do one of the following:

  - For the future secondary Server, create a certificate that is trusted in your infrastructure and that meets the requirements for custom certificates.

  - Add the self-signed certificate of the future secondary Server to the list of trusted browser certificates. We recommend that you use this option only if you cannot create a custom certificate. For the information about adding a certificate to the list of trusted certificates, refer to the documentation of your browser.

## Adding secondary Administration Server (performed on the future secondary Administration Server)

If you could not connect to the future secondary Administration Server (for example, because it was temporarily disconnected or unavailable or because the certificate file of secondary Administration Server is self-signed), you are still able to add a secondary Administration Server.

*To add as secondary an Administration Server that is not available for connection through Kaspersky Security Center Web Console:*

1. Send the certificate file of the future primary Administration Server to the system administrator of the office where the future secondary Administration Server is located. (You can, for example, write the file to an external device, such as a flash drive, or send it by email.)

   The certificate file is located on the future primary Administration Server, at /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Prompt the system administrator in charge of the future secondary Administration Server to do the following:

   a. Click the Administration Server name.

   b. On the properties page that opens, proceed to the **Hierarchy of Administration Servers** section of the **General** tab.

   c. Select the **This Administration Server is secondary in the hierarchy** option.

   d. Select the type of primary Administration Server.

   e. In the **Primary Administration Server address** field, enter the network name of the future primary Administration Server.

   f. Select the previously saved file with the certificate of the future primary Administration Server by clicking **Specify primary Administration Server certificate**.

g. If necessary, select the **Connect primary Administration Server to secondary Administration Server in DMZ** check box.

h. If the connection to the future primary Administration Server is performed through a proxy server, select the **Use proxy server** check box and specify the connection settings.

i. Click the **Save** button.

The "primary/secondary" hierarchy is built. The primary Administration Server starts receiving connection from the secondary Administration Server using port 13000. The tasks and policies from the primary Administration Server are received and applied. The secondary Administration Server is displayed on the primary Administration Server, in the administration group where it was added.

# Viewing the list of secondary Administration Servers

*To view the list of the secondary (including virtual) Administration Servers:*

1. In the main menu, select a section (except for **Marketplace**, **Console navigation**, and **Settings**).

2. At the top of the page, click the **Show hierarchy** button.

In the navigation pane that opens, the list of the secondary (including virtual) Administration Servers is displayed. You can proceed to any of these Administration Servers by clicking its name.

You cannot proceed to virtual Administration Servers if you opened the navigation pane from the **IP ranges** and **Deleted objects** sections.
The administration groups are shown, too. The groups are available for management if you opened the navigation pane from the following sections: **Managed devices**, **Policies**, **Tasks**, and **Distribution points**. Otherwise, the groups are grayed-out.

If you are connected to your primary Administration Server in Kaspersky Security Center Web Console, and can not connect to a virtual Administration Server that is managed by a secondary Administration Server, you can use one of the following ways:

- **Modify the existing installation of Kaspersky Security Center Web Console by adding the secondary Server to the list of trusted Administration Servers.** After that, you can connect to the virtual Administration Server in Kaspersky Security Center Web Console.

  1. On the device where Kaspersky Security Center Web Console is installed, run the Kaspersky Security Center Web Console installation file corresponding to the Linux distribution installed on your device under an account with administrative privileges.

     The Setup Wizard will start. Proceed through the Wizard by using the **NEXT** button.

  2. Select the **Upgrade** option.

  3. On the **Modification type** step, select the **Edit connection settings** option.

  4. On the **Trusted Administration Servers** step, add the required secondary Administration Server.

5. On the last step, click **Modify** to apply the new settings.

6. After the application reconfiguration successfully completes, click the **Finish** button.

- Use Kaspersky Security Center Web Console to connect directly to the secondary Administration Server where the virtual Server was created. Then you will be able to switch to the virtual Administration Server in Kaspersky Security Center Web Console.

# Managing virtual Administration Servers

This section describes the following actions to manage virtual Administration Servers:

- Create virtual Administration Servers
- Enable and disable virtual Administration Servers
- Assign an administrator for a virtual Administration Server
- Change the Administration Server for client devices
- Delete virtual Administration Servers

# Creating a virtual Administration Server

You can create virtual Administration Servers and add them to administration groups.

When you create a virtual Administration Server, it inherits the user list and all of the user rights of the primary Administration Server. If a user has access rights to the primary Server, this user has access rights to the virtual Server as well. After creation, you configure the access rights to the Servers independently.

*To create and add a virtual Administration Server:*

1. In the main menu, click the Administration Server name.

2. On the page that opens, proceed to the **Administration Servers** tab.

3. Select the administration group to which you want to add a virtual Administration Server.
   The virtual Administration Server will manage devices from the selected group (including the subgroups).

4. On the menu line, click **New virtual Administration Server**.

5. On the page that opens, define the properties of the new virtual Administration Server:

   - **Name of virtual Administration Server**.

   - **Administration Server connection address**.
     You can specify the name or the IP address of your Administration Server.

6. From the list of users, select the virtual Administration Server administrator. If you want, you can edit one of the existing accounts before assigning it the administrator's role, or create a new user account.

   If necessary, you can create a new account that will act as a virtual Administration Server administrator by using the kladduser utility. To do that, use the following command:

   ```
   kladduser -n <user_name> -p <password> -vs <virtual_server_name>
   ```

   where virtual_server_name is the name of the virtual Administration Server.

7. Click the **Save** button.

The new virtual Administration Server is created, added to the administration group and displayed on the **Administration Servers** tab.

If you are connected to your primary Administration Server in Kaspersky Security Center Web Console, and can not connect to a virtual Administration Server that is managed by a secondary Administration Server, you can use one of the following ways:

- **Modify the existing installation of Kaspersky Security Center Web Console by adding the secondary Server to the list of trusted Administration Servers.** After that, you can connect to the virtual Administration Server in Kaspersky Security Center Web Console.

  1. On the device where Kaspersky Security Center Web Console is installed, run the Kaspersky Security Center Web Console installation file corresponding to the Linux distribution installed on your device under an account with administrative privileges.

     The Setup Wizard will start. Proceed through the Wizard by using the **NEXT** button.

  2. Select the **Upgrade** option.

  3. On the **Modification type** step, select the **Edit connection settings** option.

  4. On the **Trusted Administration Servers** step, add the required secondary Administration Server.

  5. On the last step, click **Modify** to apply the new settings.

  6. After the application reconfiguration successfully completes, click the **Finish** button.

- Use Kaspersky Security Center Web Console to connect directly to the secondary Administration Server where the virtual Server was created. Then you will be able to switch to the virtual Administration Server in Kaspersky Security Center Web Console.

# Enabling and disabling a virtual Administration Server

When you create a new virtual Administration Server, it is enabled by default. You can disable or enable it again at any time. Disabling or enabling a virtual Administration Server is equal to switching off or on a physical Administration Server.

*To enable or disable a virtual Administration Server:*

1. In the main menu, click the Administration Server name.

2. On the page that opens, proceed to the **Administration Servers** tab.

3. Select the virtual Administration Server that you want to enable or disable.

4. On the menu line, click the **Enable / disable virtual Administration Server** button.

   The virtual Administration Server state is changed to enabled or disabled, depending on its previous state. The updated state is displayed next to the Administration Server name.

# Assigning an administrator for a virtual Administration Server

When you use virtual Administration Servers in your organization, you might want to assign a dedicated administrator for each virtual Administration Server. For example, this might be useful when you create virtual Administration Servers to manage separate offices or departments of your organization, or if you are an MSP provider and you manage your tenants through virtual Administration Servers.

When you create a virtual Administration Server, it inherits the user list and all of the user rights of the primary Administration Server. If a user has access rights to the primary Server, this user has access rights to the virtual Server as well. After creation, you configure the access rights to the Servers independently. If you want to assign an administrator for a virtual Administration Server only, make sure that the administrator does not have access rights on the primary Administration Server.

You assign an administrator for a virtual Administration Server by granting the administrator access rights to the virtual Administration Server. You can grant the required access rights in one of the following ways:

- Configure access rights for the administrator manually
- Assign one or more user roles for the administrator

To sign in to Kaspersky Security Center Web Console, an administrator of a virtual Administration Server specifies the virtual Administration Server name, user name, and password. Kaspersky Security Center Web Console authenticates the administrator and opens the virtual Administration Server to which the administrator has access rights. The administrator cannot switch between Administration Servers.

Prerequisites

Before you start, ensure that the following conditions are met:

- The virtual Administration Server is created.
- On the primary Administration Server, you have created an account for the administrator that you want to assign for the virtual Administration Server.
- You have the **Modify object ACLs** right in the **General features** → **User permissions** functional area.

Configuring access rights manually

*To assign an administrator for a virtual Administration Server:*

1. Switch to the required virtual Administration Server:

   a. In the main menu, select a section (except for **Marketplace**, **Console navigation**, and **Settings**), and then at the top of the page, click the **Show hierarchy** button.

   b. In the navigation pane that opens, click the name of the required virtual Administration Server.

   > You cannot switch to a virtual Administration Server from the **IP ranges** and **Deleted objects** sections.

   In the main menu, the Administration Server changes to the one that you selected.

2. Move to the properties of the administration Server by clicking its name in the main menu.

   Alternately, in the navigation pane, hover the mouse cursor over the name of the required virtual Administration Server, and then click the settings icon (⚙).

   The Administration Server properties window opens.

3. On the **Access rights** tab, click the **Add** button.

   A unified list of users of the primary Administration Server and the current virtual Administration Server opens.

4. From the list of users, select the account of the administrator that you want to assign for the virtual Administration Server, and then click the **OK** button.

   The application adds the selected user to the user list on the **Access rights** tab.

5. Select the check box next to the added account, and then click the **Access rights** button.

6. Configure the rights that the administrator will have on the virtual Administration Server.

   For successful authentication, at minimum, the administrator must have the following rights:

   - **Read** right in the **General features** → **Basic functionality** functional area
   - **Read** right in the **General features** → **Virtual Administration Servers** functional area

The application saves the modified user rights to the administrator account.

*To assign an administrator for multiple virtual Administration Servers:*

1. In the main menu, click the primary Administration Server name.

2. On the page that opens, proceed to the **Access rights** tab, and then click **Assign**.

   In the **Add users or groups** window that opens, select the check box near the user that you want to assign as an administrator.

3. You can switch to the **Groups** tab to select the user groups.

4. Click **Next**.

5. Select the servers to which you want to assign an administrator, and then click **Next**.

6. Select the administrator roles which you want to set for the user, if necessary.

   If you want to set custom roles for the current Administration Server for the user, go to the properties of the required Administration Server, click **Set roles**, and then select the custom roles.

7. Click **Finish** to apply the changes.

The administrator with the selected roles is now assigned to multiple virtual Administration Servers.

*To revoke the administrator access rights:*

1. Switch to the required Administration Server.

2. In the main menu, click the Administration Server name.

3. On the page that opens, proceed to the **Access rights** tab.

4. Select the check box near the user from whom you want to revoke the access rights.

5. Click **Revoke** and confirm your action.

The selected user's access rights are revoked.

## Configuring access rights by assigning user roles

Alternatively, you can grant the access rights to a virtual Administration Server administrator through user roles. For example, this might be useful if you want to assign several administrators on the same virtual Administration Server. If this is the case, you can assign the administrators' accounts the same one or more user roles instead of configuring the same user rights for several administrators.

*To assign an administrator for a virtual Administration Server by assigning user roles:*

1. On the primary Administration Server, create a new user role, and then specify all of the required access rights that an administrator must have on the virtual Administration Server. You can create several roles, for example, if you want to separate access to different functional areas.

2. Switch to the required virtual Administration Server:

   a. In the main menu, select a section (except for **Marketplace**, **Console navigation**, and **Settings**), and then at the top of the page, click the **Show hierarchy** button.

   b. In the navigation pane that opens, click the name of the required virtual Administration Server.

   > You cannot switch to a virtual Administration Server from the **IP ranges** and **Deleted objects** sections.

   In the main menu, the Administration Server changes to the one that you selected.

3. Assign the new role or several roles to the administrator account.

The application assigns the roles to the administrator account.

Configuring access rights at the object level

In addition to assigning access rights at the functional area level, you can configure access to specific objects on the virtual Administration Server, for example, to a specific administration group or a task. To do this, switch to the virtual Administration Server, and then configure the access rights in the object's properties.

# Changing the Administration Server for client devices

You can change the Administration Server that manages client devices to a different Server using the *Change Administration Server* task. After the task completion, the selected client devices will be put under the management of the Administration Server that you specify.

You cannot use the *Change Administration Server* task for client devices connected to Administration Server through connection gateways. For such devices you have to either reconfigure Network Agent or reinstall Network Agent and specify connection gateway.

*To change the Administration Server that manages client devices to a different Server:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.
3. At the **New task settings** step of the wizard, specify the following settings:

   a. In the **Application** drop-down list, select **Kaspersky Security Center**.

   b. In the **Task type** field, select **Change Administration Server**.

   c. In the **Task name** field, specify the name for the task that you are creating.

   The task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).

   d. Select devices to which the task will be assigned:

   **Assign task to an administration group**

   The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

   For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

   If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

   **Specify device addresses manually or import addresses from a list**

   You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

   You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

   **Assign task to a device selection**

The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.

4. At the **Task scope** step of the wizard, specify an administration group, devices with specific addresses, or a device selection.

5. At this step of the wizard, confirm that you agree to the terms of changing the Administration Server for client devices.

6. At this step of the wizard, select the Administration Server that you want to use to manage the selected devices:

   **Change to another primary Administration Server**

   To move client devices to another primary Administration Server, specify the following Administration Server connection settings:

   1. In the **Administration Server address** field, specify the address of the new primary Administration Server.

   2. In the **Port number** field, specify the port number to connect to Administration Server.

      The default port number is 14000.

   3. In the **SSL port** field, specify the number of the SSL port on the primary Administration Server.

      The default port number is 13000.

   4. If necessary, enable the **Use proxy server** option.

      If this option is disabled, direct connection is used to connect the device to the Administration Server.

      If this option is enabled, specify the proxy server parameters:

      - **Proxy server address**

      - **Proxy server port**

      If your proxy server requires authentication, in the **User name** and **Password** fields, specify the credentials of the account under which connection to the proxy server is established. We recommend that you specify the credentials of an account that has minimum privileges required only for the proxy server authentication.

   5. If necessary, upload a new Administration Server certificate.

   **Change to another virtual Server on this primary Server**

   Select this option to move client devices to virtual Administration Server on the current primary Administration Server. To do this, in the **Name of virtual Administration Server** drop-down list, select the necessary virtual Administration Server.

7. At the **Selecting an account to run the task** step of the wizard, specify the account settings:

   **Default account**

   The task will be run under the same account as the application that performs this task.

   By default, this option is selected.

   **Specify account**

   Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

**Account**

Account under which the task is run.

**Password**

Password of the account under which the task will be run.

8. If you want to change the default task settings, at the **Finish task creation** step of the wizard, enable the **Open task details when creation is complete** option.

   If you do not enable this option, the task will be created with the default settings. You can change the default settings later, at any time.

9. Click the **Finish** button.

   The task is created and displayed in the list of tasks.

10. Click the name of the created task to open the task properties window.

11. If you want to change the default task settings, in the task properties window, specify the general task settings according to your needs.

12. Click the **Save** button.

    The task is created and configured.

13. Run the created task.

After the task is completed, the client devices for which it was created are put under the management of the Administration Server specified in the task settings.

# Deleting a virtual Administration Server

When you delete a virtual Administration Server, all of the objects created on the Administration Server, including policies and tasks, will be deleted as well. The managed devices from the administration groups that were managed by the virtual Administration Server will be removed from the administration groups. To return the devices under management of Kaspersky Security Center Linux, run the network polling, and then move the found devices from the Unassigned devices group to the administration groups.

*To delete a virtual Administration Server:*

1. Switch to the primary physical Administration Server to which the virtual Administration Server to be deleted belongs:

   a. In the main menu, select any section (except for the **Marketplace**, **Console navigation**, and **Settings**), and then at the top of the page, click the **Show hierarchy** button.

   b. In the navigation pane that opens, click the name of the primary physical Administration Server.

      In the main menu, the Administration Server changes to the one that you selected.

2. Move to the properties of the primary physical Administration Server in one of the following ways:

   - In the navigation pane, hover the mouse cursor over the name of the required Administration Server, and then click the settings icon (⚙).

   - In the main menu, click the Administration Server name.

3. On the properties window that opens, proceed to the **Administration Servers** tab.
4. Select the virtual Administration Server that you want to delete.
5. On the menu line, click the **Delete** button.

The virtual Administration Server is deleted.

# Configuring Administration Server connection events logging

The history of connections and attempts to connect to the Administration Server during its operation can be saved to a log file. The information in the file allows you to track not only connections inside your network infrastructure, but unauthorized attempts to access the server as well.

*To log events of connection to the Administration Server:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.
2. On the **General** tab, select the **Connection ports** section.
3. Enable the **Log Administration Server connection events** setting.

All further events of inbound connections to the Administration Server, authentication results, and SSL errors will be saved to the file /var/opt/kaspersky/klnagent_srv/logs/SC.syslog.

# Setting the maximum number of events in the event repository

In the **Events repository** section of the Administration Server properties window, you can edit the settings of events storage in the Administration Server database by limiting the number of event records and record storage term. When you specify the maximum number of events, the application calculates an approximate amount of storage space required for the specified number. You can use this approximate calculation to evaluate whether you have enough free space on the disk to avoid database overflow. The default capacity of the Administration Server database is 400,000 events. The maximum recommended capacity of the database is 45 million events.

The application checks the database every 10 minutes. If the number of events reaches the specified maximum value plus 10,000, the application deletes the oldest events so that only the specified maximum number of events remains.

When the Administration Server deletes old events, it cannot save new events to the database. During this period, information about events that were rejected is written to the operating system log. The new events are queued and then saved to the database after the deletion operation is complete. By default, the event queue is limited to 20,000 events. You can customize the queue limit by editing the KLEVP_MAX_POSTPONED_CNT flag value.

*To limit the number of events that can be stored in the events repository on the Administration Server:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Events repository** section. Specify the maximum number of events stored in the database.

3. Click the **Save** button.

Additionally, you can do the following:

- Change the settings of any task to save events related to the task progress, or save only task execution results.
- Reduce or disable the storage period for the events of Administration Server, Network Agent, and Kaspersky applications installed on managed devices.

In doing so, you will reduce the number of events in the database, increase the speed of execution of scenarios associated with analysis of the event table in the database, and lower the risk that critical events will be overwritten by a large number of events.

# Moving Administration Server to another device

If you need to use Administration Server on a new device, you can move it in one of the following ways:

- Move Administration Server and the database server to a new device (the database server can be installed on the new device together with Administration Server, or on another device).
- Keep the database server on the previous device and move only Administration Server to a new device.

*To move Administration Server and the database server to a new device:*

1. On the previous device, create a backup of Administration Server data.

   To do this, you can run the data backup task through Kaspersky Security Center Web Console or run the klbackup utility.

2. On the previous device, disconnect Administration Server from the network.

3. Select a new device on which to install the Administration Server. Make sure that the hardware and software on the selected device meet the requirements for Administration Server, Kaspersky Security Center Web Console, and Network Agent. Also, check that ports used on Administration Server are available.

4. Assign the same address to the new device.

   The new Administration Server can be assigned the NetBIOS name, FQDN, and static IP address. It depends on which Administration Server address was set in the Network Agent installation package when Network Agents were deployed. Alternatively, you can use the connection address that determines the Administration Server to which Network Agent connects (you can obtain this address on managed devices by using the klnagchk utility).

5. If needed, on another device, install the database management system (DBMS) that the Administration Server will use.

   The database can be installed on the new device together with Administration Server, or on another device. Ensure that this device meets the hardware and software requirements. When you select a DBMS, consider the number of devices covered by the Administration Server.

6. Install the Administration Server on the new device.

   Note that if you move the database server to another device, specify the local address as the IP address of the device on which the database is installed (the "h" item in the Installing Kaspersky Security Center Linux instruction). If you need to keep the database server on the previous device, enter the IP address of the previous device in the "h" item of the Installing Kaspersky Security Center Linux instruction.

7. After the installation is complete, recover Administration Server data on the new device by using the klbackup utility.

8. Open Kaspersky Security Center Web Console and connect to the Administration Server.

9. Verify that all managed devices are connected to the Administration Server.

10. Uninstall the Administration Server and the database server from the previous device.

# Changing the Administration Server name

The steps for changing the server name may vary depending on your environment. You can choose one of the following scenarios to change the server name:

- Preserving connections by adding a new DNS record.
- Preserving connections by switching to an IP address-based connectivity.
- Restoring interrupted connections after changing the server name.

If you have difficulty changing the server name, contact Technical Support.

## Preserving connections by adding a new DNS record

In this scenario, managed devices and Kaspersky Security Center Web Console continue connecting to the old Administration Server address after renaming the Administration Server. To configure this, add one of the following DNS record types:

- An A record for the old Administration Server address pointing to the new Administration Server IP address.
- A CNAME record mapping the old Administration Server name to the new Administration Server name.

  For more information about configuring the required records, refer to your DNS server documentation.

*To preserve connections by adding a new DNS record:*

1. **Change the name of the Server.**

   Due to the way components are configured during installation, you cannot change the Administration Server name without reinstalling the Administration Server.

   *To change the server name:*

   1. Create a new backup of the Administration Server by using the klbackup utility.
   2. Uninstall Kaspersky Security Center Linux and Kaspersky Security Center Web Console on all administrator workstations.
   3. Manually delete the Administration Server database and the IAM database. The Administration Server does not delete it automatically during uninstallation.
   4. Rename the device in the operating system of the Administration Server, according to your OS documentation.
   5. Install the Kaspersky Security Center Linux Administration Server by using the new FQDN of the Administration Server.
   6. Restore the previously prepared Administration Server backup after installation.
   7. Check the IAM Server configuration and, if necessary, add the Administration Server address to the IAM Server configuration file.
   8. Install Web Console on all administrator workstations by specifying the new FQDN of the Administration Server in the response file.

2. Add a new DNS record for the old Administration Server address.
3. Specify the new address in the Administration Server settings in Kaspersky Security Center Web Console.
4. Run the **Change Administration Server** task on devices with direct visibility of the Administration Server. After that, managed devices will be able to connect to the Administration Server by using the new name.

   Do not run the task on devices without direct visibility of the server, otherwise they will lose connection to the Administration Server and connection gateways.

   Managed devices connected through connection gateways do not check the Administration Server name. Therefore, no additional action is required for them/. Information about the Administration Server address will not be updated in the output of the klnagchk diagnostic command.

The connection to the Administration Server is preserved after the server name is changed.

After changing the server name, the certificate information will become outdated. Since it does not affect the operation of the components, we do not recommend replacing self-signed certificates out of schedule. These certificates are generated during Kaspersky Security Center installation and renewed automatically by the server. They will be reissued with the new Administration Server name during the next automatic certificate replacement.

During the reinstallation, new certificates will be issued for the IAM server/ and Web Console server. If necessary, replace them with custom certificates issued by your Certificate Authority for the new Administration Server name. Refer to the following article for details: About Kaspersky Security Center Linux certificates.

# Preserving connections by switching to IP address-based connectivity

In this scenario, the way managed devices connect to the Administration Server is changed. Devices connect by using the Administration Server IP address instead of the Administration Server name. Switching all managed devices may take time, depending on the number of devices and how frequently they appear on the network with the Administration Server.

*To preserve connections by switching to IP address-based connectivity:*

1. **Prepare the Kaspersky Security Center infrastructure before changing the name of the Administration Server.**

   1. Connect managed devices to the Administration Server by using an IP address. After changing the name of the Administration Server, the devices that use its name for connection will be disconnected from the Server. To connect via an IP address, run the Change Administration Server task on devices with direct visibility of the Administration Server, including devices acting as connection gateways.

      Do not run the task on devices without direct visibility of the server, otherwise they will lose connection to the Administration Server and connection gateways.

      Managed devices connected through connection gateways do not check the Administration Server name. Therefore, no additional action is required for them/. Information about the Administration Server address will not be updated in the output of the klnagchk diagnostic command.

   2. Make sure that all managed devices are connected to the Administration Server via the IP address. To do this, check the following:

      - Results of the klnagchk diagnostic command in the Administration Server address line on managed devices with direct access to the Administration Server.
      - The properties information of the Network Agent installation package at the time of installation on devices.

        The Network Agent must initially be configured to connect to the Administration Server by using an IP address.

        If you install Network Agent over the existing installation without uninstalling it first, the Administration Server connection address and certificate specified in the Network Agent configuration will not be updated.

   3. Specify a new name in the existing Administration Server connection profiles.

   4. If you are using the Mobile Device Management role (managing Android and iOS devices), follow the instructions How to change the Administration Server address on mobile devices that use Kaspersky Endpoint Security for Android with the MDM or KSMM role.

2. **Change the name of the Server.**

   Due to the way components are configured during installation, you cannot change the Administration Server name without reinstalling the Administration Server.

   *To change the server name:*

   1. Create a new backup of the Administration Server by using the klbackup utility.
   2. Uninstall Kaspersky Security Center Linux and Kaspersky Security Center Web Console on all administrator workstations.
   3. Manually delete the Administration Server database and the IAM database. The Administration Server does not delete it automatically during uninstallation.
   4. Rename the device in the operating system of the Administration Server, according to your OS documentation.
   5. Install the Kaspersky Security Center Linux Administration Server by using the new FQDN of the Administration Server.
   6. Restore the previously prepared Administration Server backup after installation.
   7. Check the IAM Server configuration and, if necessary, add the Administration Server address to the IAM Server configuration file.
   8. Install Web Console on all administrator workstations by specifying the new FQDN of the Administration Server in the response file.

3. **Update the Administration Server addresses in the Administration Server settings.**

   After changing the Administration Server name, specify the new FQDN address in the Administration Server settings in Kaspersky Security Center Web Console. To do so, check and update the FQDN address in each of the following settings:

   - Kaspersky Security Network proxy server address
   - Web Server
   - Network Agent installation packages properties
   - Security code issuer name (2FA)

   In addition, do the following:

   - Specify the new server name in the policies and settings of other Kaspersky applications.
   - Republish each published stand-alone package and mobile device package.
   - Reconnect secondary Administration Servers if you use a hierarchy of Administration Servers and if the servers are connected by name and not by IP address.

4. Run the **Change Administration Server** task on devices with direct visibility of the Administration Server to change the connection address on managed devices to the new Administration Server name.

The connection to the Administration Server is preserved after the server name is changed.

After changing the server name, the certificate information will become outdated. Since it does not affect the operation of the components, we do not recommend replacing self-signed certificates out of schedule. These certificates are generated during Kaspersky Security Center installation and renewed automatically by the server. They will be reissued with the new Administration Server name during the next automatic certificate replacement.

During the reinstallation, new certificates will be issued for the IAM server/ and Web Console server. If necessary, replace them with custom certificates issued by your Certificate Authority for the new Administration Server name. Refer to the following article for details: About Kaspersky Security Center Linux certificates.

# Restoring interrupted connections after changing the server name

The scenario is relevant in the following cases:

- If you have lost the ownership of the Administration Server device's domain name but still have access to the Administration Server.
- If the Administration Server is no longer managing managed devices.
- If it is not possible to add DNS records for the old Kaspersky Security Center Linux address for other reasons.

*To restore interrupted connections after changing the server name:*

1. **Change the name of the Server.**

   Due to the way components are configured during installation, you cannot change the Administration Server name without reinstalling the Administration Server.

   *To change the server name:*

   1. Create a new backup of the Administration Server by using the klbackup utility.
   2. Uninstall Kaspersky Security Center Linux and Kaspersky Security Center Web Console on all administrator workstations.
   3. Manually delete the Administration Server database and the IAM database. The Administration Server does not delete it automatically during uninstallation.
   4. Rename the device in the operating system of the Administration Server, according to your OS documentation.
   5. Install the Kaspersky Security Center Linux Administration Server by using the new FQDN of the Administration Server.
   6. Restore the previously prepared Administration Server backup after installation.
   7. Check the IAM Server configuration and, if necessary, add the Administration Server address to the IAM Server configuration file.
   8. Install Web Console on all administrator workstations by specifying the new FQDN of the Administration Server in the response file.

2. **Update the Administration Server addresses in the Administration Server settings.**

   After changing the Administration Server name, specify the new FQDN address in the Administration Server settings in Kaspersky Security Center Web Console. To do so, check and update the FQDN address in each of the following settings:

   - Kaspersky Security Network proxy server address
   - Web Server
   - Network Agent installation packages properties
   - Security code issuer name (2FA)

   In addition, do the following:

   - Specify the new server name in the policies and settings of other Kaspersky applications.
   - Republish each published stand-alone package and mobile device package.
   - Reconnect secondary Administration Servers if you use a hierarchy of Administration Servers and if the servers are connected by name and not by IP address.

3. Restore the connection to the Administration Server on the previously managed devices:

   - On devices with direct visibility to the Administration Server, use the klmover utility to specify the connection address with the new Administration Server name. Refer to the following article for details: Connecting Network Agents to Administration Server by using the klmover utility.
   - On devices acting as connection gateways, reinstall the Network Agent and reconfigure the connection gateway role. Refer to the following article for details: Adding a connection gateway in the DMZ as a distribution point.
   - Devices connected through connection gateways will automatically reconnect after the connection gateways are restored. The Network Agent does not use the Administration Server name when connecting to connection gateways.

     Do not use the klmover utility on devices connected through connection gateways. Refer to the following article for details: Moving devices connected to Administration Server through connection gateways to another Administration Server.

   The connection to the Administration Server is restored after the server name is changed.

After changing the server name, the certificate information will become outdated. Since it does not affect the operation of the components, we do not recommend replacing self-signed certificates out of schedule. These certificates are generated during Kaspersky Security Center installation and renewed automatically by the server. They will be reissued with the new Administration Server name during the next automatic certificate replacement.

During the reinstallation, new certificates will be issued for the IAM server/ and Web Console server. If necessary, replace them with custom certificates issued by your Certificate Authority for the new Administration Server name. Refer to the following article for details: About Kaspersky Security Center Linux certificates.

# Changing DBMS credentials

Sometimes, you may need to change DBMS credentials, for example, in order to perform a credential rotation for security purposes.

## Changing the Administration Server database credentials

*To change Administration Server and IAM database credentials in a Linux environment:*

1. Stop Administration Server. Depending on the deployment type of Kaspersky Security Center Linux, run one of the following commands under the root account:

   - For a Kaspersky Security Center Linux failover cluster:

     On the active node, run the following command:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc
     ```

   - For a geo-distributed Kaspersky Security Center Linux failover cluster:

     On both nodes, run the following command:

     ```
     crm node standby
     ```

   - For a non-cluster Administration Server deployment:

     Run the following commands:

     ```
     systemctl stop kladminserver_srv.service
     systemctl stop kliam_srv.service
     ```

2. Connect to the Administration Server database with DBMS superuser privileges and run the following command:

   ```
   REASSIGN OWNED BY <old_kscdbadmin> TO <new_kscdbadmin>;
   ```

   where `<old_kscdbadmin>` is the old DBMS user account that the Administration Server used to connect to its database, and `<new_kscdbadmin>` is the new DBMS user account.

3. Connect to the IAM database with DBMS superuser privileges and run the following command:

   ```
   REASSIGN OWNED BY <old_iamdbadmin> TO <new_iamdbadmin>;
   ```

   where `<old_iamdbadmin>` is the previous DBMS account used by the Administration Server to connect to its database, and `<new_iamdbadmin>` is the new DBMS accounts.

4. Locate the IAM configuration file: /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml

5. In the `dbms_iam` section, specify new account credentials in the user and password fields. Ensure that the account exists in the DBMS and is specified as the IAM database owner.

6. Run Administration Server. Depending on the deployment type of Kaspersky Security Center Linux, run one of the following commands under the root account:

   - For a Kaspersky Security Center Linux failover cluster:

     On the active node, run the following command:

     ```
     /opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc
     ```

   - For a geo-distributed Kaspersky Security Center Linux failover cluster:

     On both nodes, run the following command:

     ```
     crm node online
     ```

   - For a non-cluster Administration Server deployment:

     Run the following commands:

     ```
     systemctl start kladminserver_srv.service
     systemctl start kliam_srv.service
     ```

7. Run the klsrvconfig utility:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

8. Specify a new account name. You should specify credentials of an account that exists in the DBMS.

9. Enter a new password.

10. Specify the new password for confirmation.

11. Wait until the Administration Server resumes operation and a syslog entry on the active node appears stating that the Administration Server is ready for GUI operations.

The Administration Server database credentials are changed.

# Backup copying and restoration of the Administration Server data

Data backup allows you to move Administration Server from one device to another without data loss. Through backup, you can restore data when moving the Administration Server database to another device, or when upgrading to a newer version of Kaspersky Security Center. Also, you can use data backup to move Administration Server data from Kaspersky Security Center Windows under management of Kaspersky Security Center Linux (moving data from Kaspersky Security Center Linux to Kaspersky Security Center Windows is not supported).

The installed management plug-ins are not backed up. After you restore Administration Server data from a backup copy, you need to download and reinstall plug-ins for managed applications.

Before you back up the Administration Server data, perform the following actions:

- **Follow requirements for creating a backup on Administration Server 16 or earlier and restoring it on version 16.1 or later**

  - If you create a data backup on Administration Server 16 or earlier and restore it on Administration Server 16.1 or later, two-factor authentication is enabled. For more information, refer to About two-factor authentication for an account.

    To ensure that users can sign in to Web Console with their existing accounts by using configured two-factor authentication secret keys, and that OpenAPI automation scripts continue to work after the restore, you must perform the following steps:

    - Enable two-factor authentication for all users
    - Administrators must configure two-factor authentication for their own accounts
    - Excluding accounts from two-factor authentication

      If needed, add integration accounts used to run scripts through OpenAPI to the exclusion list.

    If it is not possible to configure two-factor authentication before creating the backup, user accounts will be added to the two-factor authentication allow list and will be able to configure two-factor authentication when signing in to the Web Console. More detailed conditions for adding an account to the allow list are described in the topic Allowing users to configure two-factor authentication.

- Check whether a virtual Administration Server is added to the administration group. If a virtual Administration Server is added, make sure that an administrator is assigned to this virtual Administration Server before the backup. You cannot grant the administrator access rights to the virtual Administration Server after the backup. Note that if the administrator account credentials are lost, you will not be able to assign a new administrator to the virtual Administrator Server.

- If you want to backup or restore a Kaspersky Security Center Linux failover cluster, you must stop the entire cluster for maintenance and then restart it when backup or restoration is completed.

You can create a backup copy of Administration Server data in one of the following ways:

- By creating and running a data backup task through Kaspersky Security Center Web Console.
- By running the klbackup utility on the device that has Administration Server installed. This utility is included in the Kaspersky Security Center distribution kit. After the installation of Administration Server, the utility is located in the root of the destination folder specified at the application installation (usually, /opt/kaspersky/ksc64/sbin/klbackup).

The following data is saved in the backup copy of Administration Server:

- Database of the Administration Server (policies, tasks, application settings, events saved on the Administration Server)
- Configuration details of the structure of administration groups and client devices
- Repository of distribution packages of applications for remote installation
- Administration Server certificate
- Two-factor authentication secret keys configured for user accounts
- List of user accounts excluded from two-factor authentication

You can create a backup copy of Administration Server data either by creating and running a data backup task or by using the klbackup utility. Restoration of Administration Server data is only possible by using the klbackup utility. You must perform the restoration on an operable instance of Administration Server that has just been installed and has the same version (or later) for which the backup copy was created. Do not use any third-party tools for backup or restoration, and if possible, do not remove the previous Kaspersky Security Center Linux installation until the configuration and data transfer are fully completed.

# Creating an Administration Server data backup task

Backup tasks are Administration Server tasks; they are created through the quick start wizard. If a backup task created by the quick start wizard has been deleted, you can create one manually.

The *Backup of Administration Server data* task can only be created in a single copy. If the Administration Server data backup task has already been created for the Administration Server, it is not displayed in the task type selection window.

*To create an Administration Server data backup task:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.
3. In the **Application** list, select **Kaspersky Security Center 17**, and in the **Task type** list, select **Backup of Administration Server data**.

4. On the corresponding step, specify the following information:

   - Folder for storage of backup copies
   - Password for the backup (optional)
   - Maximum number of backup copies to save

5. If you want to modify the default task settings, enable the **Finish task creation** option at the **Open task details when creation is complete** step. If you do not enable this option, the task is created with the default settings. You can change the default settings later, at any time.

6. Click the **Finish** button.

   The task is created and displayed in the list of tasks.

# Using the klbackup utility to back up and recover data

You can copy Administration Server data for backup and future recovery using the klbackup utility, which is part of the Kaspersky Security Center distribution kit.

The instance of Administration Server on which the restoration is to be performed, must use a DBMS of the same type. The version of Administration Server can be the same (with an identical or later patch), or later.

If you backed up data of Administration Server included in Kaspersky Security Center Linux 15 or earlier when using the MariaDB DBMS of an earlier version, and then recover data on a device with a later version of MariaDB, an error may occur. For more information, refer to How to restore Administration Server data from a backup created on an earlier DBMS version.

Network agent flags are not restored when you use the klbackup utility. You need to configure network agent flags manually.

*To create a backup copy or recover Administration Server data in silent mode,*

Run klbackup with the required set of keys from the command line of the device that has Administration Server installed.

Utility command line syntax:

```
klbackup -path <backup path> [-linux_path <DBMS backup path>-node_cert <certificate path>] [-logfile <log file> [-use_ts]|[-restore] [-password <password>] [-cert_only]
```

If no password is specified in the command line of the klbackup utility, the utility prompts you to enter the password interactively.

Descriptions of the keys:

- `-path <backup path>`—Save information in the backup folder, or use data from the backup folder for recovery (mandatory parameter).

- `-linux_path <DBMS backup path>`—Local path to folder with DBMS backup data.

  The database server account and the klbackup utility should be granted permissions for changing data in the DBMS backup folder.

- `-node_cert <certificate path>`—Server certificate file to configure inactive failover cluster node after recovery. If not set, it will be automatically retrieved from the Server.

- `-logfile <log file>`—Save a report about Administration Server data backup and recovery.

  The database server account and the klbackup utility should be granted permissions for changing data in the backup folder.

- `-use_ts`—When saving data, copy information to the backup folder, to the subfolder with a name in the `klbackup YYYY-MM-DD # HH-MM-SS` format, which includes the current date and operation time in UTC. If no key is specified, information is saved in the root of the backup folder.

  During attempts to save information in a folder that already stores a backup copy, an error message appears. No information will be updated.

  Availability of the `-use_ts` key allows an Administration Server data archive to be maintained. For example, if the `-path` key indicates the folder `/tmp/KLBackups`, the folder `klbackup 2022/6/19 # 11-30-18` then stores information about the status of the Administration Server as of June 19, 2022, at 11:30:18 AM.

- `-restore`—Recover Administration Server data. Data recovery is performed based on information contained in the backup folder. If no key is available, data is backed up in the backup folder.

- `-password <password>`—Password to protect the sensitive data.

  A forgotten password cannot be recovered. There are no password requirements. The password length is unlimited and zero length (no password) is also possible.

  When restoring data, you must specify the same password that was entered during backup. If the path to a shared folder changed after backup, check the operation of tasks that use restored data (restore tasks and remote installation tasks). If necessary, edit the settings of these tasks. While data is being restored from a backup file, no one must access the shared folder of Administration Server. The account under which the klbackup utility is started must have full access to the shared folder. To restore the Administration Server data from the backup, we recommend that you run the utility on a newly installed Administration Server.

- `-cert_only`—Save or recover only the certificate and private key of Administration Server.

  This flag can be useful when you perform the migration from Administration Server of Kaspersky Security Center Windows to Administration Server of Kaspersky Security Center Linux. Also, you can migrate managed devices between Kaspersky Security Center Linux Administration Servers, as well as between Kaspersky Security Center Windows Administration Servers.

You can use a data backup to migrate Kaspersky Security Center Windows Administration Server data to be managed by Kaspersky Security Center Linux.
If you use MySQL or MariaDB as a DBMS for Kaspersky Security Center Windows and for Kaspersky Security Center Linux, the `lower_case_table_names` parameter must match for the current and new DBMSs. Before creating a backup copy of the data, check the `lower case table names` setting. Then when installing MySQL or MariaDB for Kaspersky Security Center Linux, you must set the `lower_case_table_names` parameter to the same value as specified for this parameter for Windows.

If, during restoration, the Administration Server common certificate is replaced with another certificate from a backup, perform the following steps to ensure proper operation:
1. Reinstall the Web Console to avoid the following error:
*Administration Server uses an untrusted certificate. Please reconfigure the application by specifying a valid certificate, or contact the main administrator*.
2. Check the IAM Server configuration and, if necessary, add the Administration Server address to the IAM Server configuration file.

# Using the klbackup utility to switch managed devices under management of another Administration Server

The klbackup utility allows you to switch managed devices under management of another Administration Server. You can change the Kaspersky Security Center Windows Administration Server to Kaspersky Security Center Linux Administration Server by using the klbackup utility when you perform the migration. Also, you can migrate managed devices between Kaspersky Security Center Linux Administration Servers, as well as between Kaspersky Security Center Windows Administration Servers.

Before you start, **check the requirements to a custom certificate**.

If you are using custom certificate instead of the self-signed one, before upgrading Kaspersky Security Center Linux to the later version, you have to make sure that the certificate includes the Subject Alternative Name (SAN). If not, is important to replace the certificate before upgrading Kaspersky Security Center Linux. Otherwise, you will not be able to sign in to Web Console after upgrade.

*To make sure that the certificate includes SAN:*

1. On the device with Administration Server installed, execute the command:

   - For a Linux-based device:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - For a Windows-based device:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Make sure that the Subject Alternative Name (SAN) is present in the command output and contains the address of the Administration Server device.

3. If the Subject Alternative Name is missing, use the klsetsrvcert utility to replace your user certificate with a certificate that meets the requirements.

*To switch managed devices under management of another Administration Server by using the klbackup utility:*

1. On the previous device, create a backup copy of the Administration Server certificate and private key.

   You can create a backup copy in one of the following ways:

   - By using the klbackup utility interface (only for Kaspersky Security Center Windows Administration Server)

     Run the klbackup utility located in the Kaspersky Security Center installation folder, and then create a backup by using the **Restore or back up Administration Server certificate only** option.

   - By using the command prompt (for Kaspersky Security Center Windows and Kaspersky Security Center Linux Administration Servers version 15.1 or later)

     Run the klbackup utility with the `-cert_only` key from the command line, to create a backup copy of the Administration Server certificate and private key:

     ```
     klbackup -path <path to the backup copy of Administration Server certificate> -cert_only
     ```

2. On the previous device, disconnect Administration Server from the network.

3. Assign the same domain name to the device with another Administration Server.

   The new Administration Server can be assigned the NetBIOS name, FQDN, and static IP address. It depends on which Administration Server address was set in the Network Agent installation package when Network Agents were deployed. Alternatively, you can use the connection address that determines the Administration Server to which Network Agent connects (you can obtain this address on managed devices by using the klnagchk utility).

   If it is impossible to assign the same address to the device with another Administration Server, you must generate a new Administration Server certificate and specify this certificate in the IAM configuration file. After installation of the Administration Server you need to manually switch Network Agents to the new Administration Server.

4. On a device with another Administration Server, restore the Administration Server certificate and private key from the backup copy.

   You can restore a backup copy in one of the following ways:

   - By using the klbackup utility interface (only for Kaspersky Security Center Windows Administration Server)

     Run the klbackup utility, and then restore a backup by using the **Restore or back up Administration Server certificate only** option.

- By using the command prompt (for Kaspersky Security Center Windows and Kaspersky Security Center Linux Administration Servers version 15.1 or later)

  Run the `klbackup` utility with the `-cert_only` option from the command line to restore the Administration Server certificate and private key from a backup copy:

  ```
  klbackup -path <path to the backup copy of Administration Server certificate> -restore -cert_only
  ```

5. Configure certificate verification by Administration Server and IAM Server.

   Managed devices are put under the management of another Administration Server. You can go to this Administration Server and ensure that managed devices are visible in the network, and that Network Agent is installed and running on them (the *Yes* value in the **Visible**, **Network Agent is installed**, and **Network Agent is running** columns).

# Backup and restoring Administration Server data when using MySQL or MariaDB

You can use a data backup to migrate Administration Server data from Kaspersky Security Center Windows under management of Kaspersky Security Center Linux. Migration by using Administration Server data backup is supported only for migration to Kaspersky Security Center Linux 15.2 or later from any supported version of Kaspersky Security Center Windows.

If you use MySQL or MariaDB as a DBMS for Kaspersky Security Center Windows and for Kaspersky Security Center Linux, the `lower_case_table_names` parameter must match for the current and new DBMSs. Otherwise, Administration Server data will be migrated incorrectly.

Before you backup Administration Server data on Kaspersky Security Center Windows, check the `lower_case_table_names` parameter value. If you do not specify this parameter during the DBMS installation earlier, the default parameter value is used. The default value of the `lower_case_table_names` parameter for Windows is `1`.

Then when installing MySQL or MariaDB for Kaspersky Security Center Linux, set the same value for `lower_case_table_names` as specified for this parameter for Windows. For details, refer to the instructions from the MySQL website. If you do not specify this parameter, the default parameter value is used. For Linux-based operating systems, the default value of the `lower_case_table_names` parameter is different from the default value for Windows.

If you want to install MySQL 8.0, specifying the `lower_case_table_names` parameter according to this instruction may not work. In this case, you must first install MySQL 5.7, specify the `lower_case_table_names` parameter by using the instruction, and then upgrade MySQL 5.7 to MySQL 8.0. If the `lower_case_table_names` parameter does not match for the current and new DBMSs, Administration Server data will be restored incorrectly.

# Administration Server maintenance

The Administration Server maintenance allows you to free up space in the folder of the Administration Server and reduce the database volume by deleting objects that are no longer needed. This helps you to improve the performance and operation reliability of the application. We recommend that you maintain Administration Server at least every week.

The Administration Server maintenance is performed using the dedicated task. The application performs the following actions when maintaining the Administration Server:

- Deletes unnecessary folders and files from the storage folder.
- Deletes unnecessary records from tables (also known as "dangling pointers").
- Clears the cache.
- Maintains the database (if you use PostgreSQL as a DBMS):
  - Re-organizes database indexes
  - Updates the database statistics
  - Shrinks the database (if necessary)

The Administration Server maintenance task supports MariaDB versions 10.3 and later. If you use MariaDB versions 10.2 or earlier, administrators have to maintain this DBMS on their own.

The Administration Server maintenance task is created automatically when the Administration Server is started. If the Administration Server maintenance task is deleted, you can create it manually.

*To create the Administration Server maintenance task:*

1. In the main menu, go to **Tasks**.
2. Click the **Add** button.
   The New task wizard starts.
3. In the **New task settings** window of the wizard, select **Administration Server maintenance** as the task type and click the **Next** button.
4. Follow the rest of the wizard instructions.

The newly created task is displayed in the list of tasks. Only one Administration Server maintenance task can be running for a single Administration Server. If an Administration Server maintenance task has already been created for an Administration Server, no new Administration Server maintenance task can be created.

# Deleting a hierarchy of Administration Servers

If you no longer want to have a hierarchy of Administration Servers, you can disconnect them from this hierarchy.

*To delete a hierarchy of Administration Servers:*

1. In the main menu, click the Administration Server name.
2. On the page that opens, proceed to the **Administration Servers** tab.
3. In the administration group from which you want to delete the secondary Administration Server, select the secondary Administration Server.

4. On the menu line, click **Delete**.

5. In the window that opens, click **OK** to confirm that you want to delete the secondary Administration Server.

   The former primary Administration Server and the former secondary Administration Server are now independent of each other. The hierarchy no longer exists.

# Access to public DNS servers

If access to Kaspersky servers by using the system DNS is not possible, Kaspersky Security Center Linux can use the following public DNS servers, in the following order:

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)

Requests to these DNS servers may contain domain addresses and the public IP address of the Administration Server, because the application establishes a TCP/UDP connection to the DNS server. If Kaspersky Security Center Linux is using a public DNS server, data processing is governed by the privacy policy of the relevant service.

*To configure the use of public DNS by using the klscflag utility:*

1. Run the command line, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.

2. To disable the use of public DNS, run the following command under the root account:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. To enable the use of public DNS, run the following command under the root account:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

# Configuring the interface

You can configure the Kaspersky Security Center Web Console interface to display and hide sections and interface elements, depending on the features being used.

*To configure the Kaspersky Security Center Web Console interface in accordance with the currently used set of features:*

1. In the main menu, go to **Settings** → **Interface options**.
2. Enable or disable the required options:
   - **Show data encryption and protection**
   - **Show MDR features**
   - **Show EDR alerts**
3. Click the **Save** button.

After the required options are enabled, the console displays the corresponding sections in the main menu. For example, if you enable **Show EDR alerts**, the **Monitoring** → **Alerts** section appears in the main menu.

# Encrypted connection to an Administration Server

Data exchange between client devices and Administration Server can be performed using the TLS (Transport Layer Security) protocol. The TLS protocol can identify the interacting parties, encrypt the data that is transferred, and protect data against modification during transfer. The TLS protocol uses public keys to authenticate the interacting parties and encrypt data.

When a client device connects to Administration Server for the first time, Network Agent on the device downloads a copy of the Administration Server certificate and stores it locally.

If you install Network Agent on a device locally, you can select the Administration Server certificate manually.

The downloaded copy of the certificate is used to verify Administration Server rights and permissions during subsequent connections.

During future sessions, Network Agent requests the Administration Server certificate at each connection of the device to Administration Server and compares it with the local copy. If the copies do not match, the device is not allowed access to Administration Server.

# Encrypt communication with TLS

To fix vulnerabilities on your organization's corporate network, you can enable traffic encryption by using the TLS protocol. You can enable TLS encryption protocols and supported cipher suites on Administration Server. Kaspersky Security Center Linux supports the TLS protocol versions 1.0, 1.1, 1.2, and 1.3. You can select the required encryption protocol and cipher suites.

Kaspersky Security Center Linux uses self-signed certificates. You can also use your own certificates. We recommend using certificates issued by trusted certificate authorities.

*To configure allowed encryption protocols and cipher suites on Administration Server:*

1. Run the command line, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.

2. Use the SrvUseStrictSslSettings flag to configure allowed encryption protocols and cipher suites on Administration Server. Execute the following command in the command line under the root account:

   ```
   ./klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <value> -t d
   ```

   Specify the <value> parameter of the SrvUseStrictSslSettings flag:

   - 4—Only the TLS 1.2 and TLS 1.3 protocols are enabled. Also, cipher suites with TLS_RSA_WITH_AES_256_GCM_SHA384 are enabled (these cipher suites are needed for backward compatibility with the previous versions of Kaspersky Security Center Linux). This is the default value.

     Cipher suites supported for the TLS 1.2 protocol:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (cipher suite with TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Cipher suites supported for the TLS 1.3 protocol:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - 5—Only the TLS 1.2 and TLS 1.3 protocols are enabled. For the TLS 1.2 and TLS 1.3 protocols, the specific cipher suites listed below are supported.

     Cipher suites supported for the TLS 1.2 protocol:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

Cipher suites supported for the TLS 1.3 protocol:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

We do not recommend using 0, 1, 2, or 3 as the parameter value of the SrvUseStrictSslSettings flag. These parameter values correspond to insecure TLS protocol versions (TLS 1.0 and TLS 1.1) and insecure cipher suites, and are used only for backward compatibility with earlier Kaspersky Security Center versions.

3. Restart the following Kaspersky Security Center Linux services:
   - Administration Server
   - Web Server
   - Activation Proxy

As a result, traffic encryption by using the TLS protocol is enabled.

You can use the KLTR_TLS12_ENABLED and KLTR_TLS13_ENABLED flags to enable the support of the TLS 1.2 and TLS 1.3 protocols, respectively. These flags are enabled by default.

*To enable or disable the support of the TLS 1.2 and TLS 1.3 protocols:*

1. Run the klscflag utility.

   Run the command line, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.

2. Execute one of the following commands in the command line under the root account:
   - Use this command to enable or disable the support of the TLS 1.2 protocol:

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <value> -t d
     ```

   - Use this command to enable or disable the support of the TLS 1.3 protocol:

     ```
     ./klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <value> -t d
     ```

   Specify the `<value>` parameter of the flag:

   - `1`—To enable the support of the TLS protocol.
   - `0`—To disable the support of the TLS protocol.

# Network settings for interaction with external services

Kaspersky Security Center Linux uses the following network settings for interacting with external services.

Network settings

| Network settings | Address | Description |
|---|---|---|
| Port: 443<br>Protocol: HTTPS | `https://activation-v2.kaspersky.com` | Application activation. |
| Port: 443<br>Protocol: HTTPS | `https://products.s.kaspersky-labs.com` | Repository of distribution packages of applications for remote installation |
| Port: 443<br>Protocol: HTTPS | `https://s00.upd.kaspersky.com`<br>`https://s01.upd.kaspersky.com`<br>`https://s02.upd.kaspersky.com`<br>`https://s03.upd.kaspersky.com`<br>`https://s04.upd.kaspersky.com`<br>`https://s05.upd.kaspersky.com`<br>`https://s06.upd.kaspersky.com`<br>`https://s07.upd.kaspersky.com`<br>`https://s08.upd.kaspersky.com`<br>`https://s09.upd.kaspersky.com`<br>`https://s10.upd.kaspersky.com`<br>`https://s11.upd.kaspersky.com`<br>`https://s12.upd.kaspersky.com`<br>`https://s13.upd.kaspersky.com`<br>`https://s14.upd.kaspersky.com`<br>`https://s15.upd.kaspersky.com`<br>`https://s16.upd.kaspersky.com`<br>`https://s17.upd.kaspersky.com`<br>`https://s18.upd.kaspersky.com`<br>`https://s19.upd.kaspersky.com`<br>`https://cm.k.kaspersky-labs.com` | Updating Kaspersky databases, software modules, and applications. |
| Port: 443<br>Protocol: HTTPS | `https://downloads.upd.kaspersky.com` | • Updating Kaspersky databases, software modules, and applications.<br>• Checking if Kaspersky servers are accessible.<br>Before downloading Kaspersky databases and software modules, Kaspersky Security Center Linux checks if Kaspersky servers are accessible. If access to the servers using system DNS is not possible, the application uses public DNS servers. |

| Network settings | Address | Description |
| --- | --- | --- |
| Port: 80<br>Protocol: HTTP | http://p00.upd.kaspersky.com<br>http://p01.upd.kaspersky.com<br>http://p02.upd.kaspersky.com<br>http://p03.upd.kaspersky.com<br>http://p04.upd.kaspersky.com<br>http://p05.upd.kaspersky.com<br>http://p06.upd.kaspersky.com<br>http://p07.upd.kaspersky.com<br>http://p08.upd.kaspersky.com<br>http://p09.upd.kaspersky.com<br>http://p10.upd.kaspersky.com<br>http://p11.upd.kaspersky.com<br>http://p12.upd.kaspersky.com<br>http://p13.upd.kaspersky.com<br>http://p14.upd.kaspersky.com<br>http://p15.upd.kaspersky.com<br>http://p16.upd.kaspersky.com<br>http://p17.upd.kaspersky.com<br>http://p18.upd.kaspersky.com<br>http://p19.upd.kaspersky.com<br>http://downloads0.kaspersky-labs.com<br>http://downloads1.kaspersky-labs.com<br>http://downloads2.kaspersky-labs.com<br>http://downloads3.kaspersky-labs.com<br>http://downloads4.kaspersky-labs.com<br>http://downloads5.kaspersky-labs.com<br>http://downloads6.kaspersky-labs.com<br>http://downloads7.kaspersky-labs.com<br>http://downloads8.kaspersky-labs.com<br>http://downloads9.kaspersky-labs.com<br>http://downloads.kaspersky-labs.com<br>http://cm.k.kaspersky-labs.com | Updating Kaspersky databases, software modules, and applications. |
| Port: 443<br>Protocol: HTTPS | https://ds.kaspersky.com<br>https://dc1.ksn.kaspersky-labs.com<br>https://dc1-file.ksn.kaspersky-labs.com<br>https://dc1-pp.ksn.kaspersky-labs.com<br>https://dc1-st.ksn.kaspersky-labs.com/<br>https://dc1-cert.ksn.kaspersky-labs.com<br>https://dc1-cf.ksn.kaspersky-labs.com<br>https://dc1-file.ksn.kaspersky-labs.com<br>https://dc1-kas.ksn.kaspersky-labs.com<br>https://dc1-ml.ksn.kaspersky-labs.com<br>https://dc1-pp.ksn.kaspersky-labs.com<br>https://dc1-st.ksn.kaspersky-labs.com<br>https://dc1.ksn.kaspersky-labs.com | Using Kaspersky Security Network. |

| Network settings | Address | Description |
| --- | --- | --- |
| Port: 443, 1443<br>Protocol: HTTPS | https://ksn-file-geo.kaspersky-labs.com<br>https://ksn-verdict-geo.kaspersky-labs.com<br>https://ksn-url-geo.kaspersky-labs.com<br>https://ksn-a-p2p-geo.kaspersky-labs.com<br>https://ksn-info-geo.kaspersky-labs.com<br>https://ksn-cinfo-geo.kaspersky-labs.com | Using Kaspersky Security Network. |
| Port: 443, 1443<br>Protocol: KSN | ksn://ksn-a-p2p-geo.kaspersky-labs.com<br>ksn://ksn-a-stat-geo.kaspersky-labs.com<br>ksn://ksn-ca-geo.kaspersky-labs.com<br>ksn://ksn-cinfo-geo.kaspersky-labs.com<br>ksn://ksn-crypto-catm-geo.kaspersky-labs.com<br>ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com<br>ksn://ksn-crypto-hash-geo.kaspersky-labs.com<br>ksn://ksn-crypto-ipm-geo.kaspersky-labs.com<br>ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com<br>ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com<br>ksn://ksn-eu-stat-kmp.kaspersky-labs.com<br>ksn://ksn-file-geo.kaspersky-labs.com<br>ksn://ksn-his-geo.kaspersky-labs.com<br>ksn://ksn-info-geo.kaspersky-labs.com<br>ksn://ksn-kas-geo.kaspersky-labs.com<br>ksn://ksn-kddi.kaspersky-labs.com<br>ksn://ksn-ml-geo.kaspersky-labs.com<br>ksn://ksn-oui-geo.kaspersky-labs.com<br>ksn://ksn-pp.kaspersky-labs.com<br>ksn://ksn-src.kaspersky-labs.com<br>ksn://ksn-stat-geo.kaspersky-labs.com<br>ksn://ksn-tcert-geo.kaspersky-labs.com<br>ksn://ksn-url-geo.kaspersky-labs.com<br>ksn://ksn-verdict-geo.kaspersky-labs.com<br>ksn://mdr.ksn.kaspersky-labs.com<br>ksn://stat-eu.ksn.kaspersky-labs.com<br>ksn://stat-hq.ksn.kaspersky-labs.com<br>ksn://stat-ru.ksn.kaspersky-labs.com<br>ksn://stat-sa.ksn.kaspersky-labs.com<br>ksn://stat-sbr.ksn.kaspersky-labs.com | Using Kaspersky Security Network. |
| Port: 443<br>Protocol: HTTPS | https://click.kaspersky.com<br>https://redirect.kaspersky.com | Following links from the interface. |

| Network settings | Address | Description |
|---|---|---|
| Port: 80<br>Protocol: HTTP | `http://crl.kaspersky.com`<br>`http://ocsp.kaspersky.com` | These servers are part of the Public Key Infrastructure (PKI) and are necessary to verify the validity status of the Kaspersky digital signature certificates. The CRL is a list of revoked certificates. The OCSP allows you to request the status of a specific certificate in real time. These servers help to ensure the security of interaction with digital certificates and protect against possible attacks. |
| Port: 443<br>Protocol: HTTPS | `https://ipm-klca.kaspersky.com` | Marketing announcements |
| Port: 443<br>Protocol: HTTPS | `https://tip.kaspersky.com` | Responding to threats through Kaspersky Threat Intelligence Portal (when using the Kaspersky Next XDR Optimum functionality). |
| Port: 443<br>Protocol: HTTPS | For the full list of addresses, refer to the Address and domain structure article | Responding to threats through Kaspersky Automated Security Awareness Platform (when using the Kaspersky Next XDR Optimum functionality). |

For proper interaction of Kaspersky Security Center Linux with external services, consider the following recommendations:
- Unencrypted network traffic must be allowed on ports 443 and 1443 on the network equipment and proxy server of your organization.
- When Administration Server interacts with Kaspersky update servers and Kaspersky Security Network servers, it is necessary to avoid hijacking network traffic with certificate substitution (MITM attacks).

*To download updates through the HTTP or HTTPS protocol by using the klscflag utility:*

1. Run the command line, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.

2. If you want to download updates through the HTTP protocol, run one of the following commands under the root account:

   - On the device with Administration Server installed:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - On a distribution point:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   If you want to download updates through the HTTPS protocol, run one of the following commands under the root account:

   - On the device with Administration Server installed:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - On a distribution point:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

# Global list of subnets

For each Administration Server you use, you can set up a global list of subnets to store the information about subnets of your network. This list helps you match pairs {IP address, mask} and physical units such as branch offices. You can use subnets from this list in the networking rules and settings.

*To add a subnet to the global list of subnets:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Global subnets** section.

3. Click **Add**.

   The **New subnet** window opens.

4. Fill in the following fields:

   - **Name**
   - **Subnet address**
   - **Subnet mask**
   - **Description**

5. Click the **Save** button.

   The window is closed, and the subnet appears in the list of subnets.

If necessary, in the list of global subnets you can do the following:

- Delete subnets from the list by selecting the required subnet and clicking the **Remove** button.
- Modify the properties of subnets by clicking the link with name of the required subnet, and then performing the actions described in steps 4–5.

# Checking the integrity of modules by using the klscmodchk and integrity_checker utilities

Kaspersky Security Center Linux contains multiple binary modules in the form of dynamically linked libraries, executable files, configuration files, and interface files. An attacker might replace one or more executable modules or application files with other files that contain malicious code. To prevent the spoofing of modules and files, Kaspersky Security Center Linux implements a component integrity check using the klscmodchk and integrity_checker utilities. These utilities check modules and files for unauthorized changes or damage. If a module or application file has an incorrect checksum, it is considered damaged.

The klscmodchk utility performs integrity checks for the following Kaspersky Security Center Linux components:

- Administration Server
- Network Agent

The integrity_checker utility performs integrity checks for the following Kaspersky Security Center Linux components:

- Administration Server
- Network Agent
- Kaspersky Security Center Web Console

Both utilities check module integrity based on the kl_file_integrity_manifest.xml manifest file, which is part of the Kaspersky Security Center Linux build and is located in the installation folder. The component manifest file contains files whose integrity is important for the correct operation of the Kaspersky Security Center Linux component. The integrity of the manifest files themselves is also checked.

It is strongly not recommended to modify the kl_file_integrity_manifest.xml manifest file, as this will invalidate the digital signature and cause the integrity check to fail.

To check the integrity of the Kaspersky Security Center Linux component, run one of the following commands:

- `klscmodchk [ parameters ]`

  The klscmodchk utility launches the integrity_checker utility with the `--verbose` parameter and checks the integrity of the modules.

  Parameters for the klscmodchk utility:

  - `-logfile < log_file_path >`—Specify the path to a file on the disk for logging. By default, information is output to the console.
  - `-verbose`—Output extended information during integrity checking.

- `integrity_checker [ parameters ] < manifest_file_path >`

  Parameters for the integrity_checker utility:

  - `--help`—Display the integrity_checker utility help.
  - `--version`—Display the integrity_checker utility version.
  - `--verbose`—Display information about the utility's operation. When performing an integrity check, it is sufficient to use this parameter in the command.

The result of checking each manifest file is displayed next to the manifest file name in the following format:

- SUCCEEDED—File integrity confirmed (return code 0).
- FAILED—File integrity not confirmed (non-zero return code).

You can also configure integrity checks to launch automatically when you launch the application. By default, automatic integrity checking is disabled.

*To enable automatic integrity checking:*

1. On the device where Administration Server is installed, at the command prompt, enter the following command:

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Restart the device.

   The automatic integrity checking is enabled.

At the next run of Kaspersky Security Center, the klscmodchk utility will run together with Administration Server, and start the modules integrity checking. The result of integrity checks are written to the Kaspersky Event Log.

# Discovering networked devices

This section describes search and discovery of networked devices.

Kaspersky Security Center Linux allows you to find devices on the basis of specified criteria. You can save search results to a text file.

The search and discovery feature allows you to find the following devices:

- Managed devices in administration groups of Open Single Management Platform Administration Server and its secondary Administration Servers.
- Unassigned devices managed by Administration Server and its secondary Administration Servers.

# Scenario: Discovering networked devices

You must perform device discovery before installation of the security applications. When all networked devices are discovered, you can receive information about them and manage them through policies. Regular network polls are needed to discover if there are any new devices and whether previously discovered devices are still on the network.

Discovery of networked devices proceeds in stages:

1. **Initial device discovery**

   When you complete the quick start wizard, perform device discovery manually.

2. **Configuring future polls**

   Make sure that IP range polling is enabled and that the poll schedule meets the needs of your organization. When configuring the poll schedule, use the recommendations for network polling frequency.

   You can also enable Zeroconf polling if your network includes IPv6 devices.

   If networked devices are included in a domain, it is recommended to use domain controller polling.

   Use Windows-based distribution points to poll Windows networks.

3. **Setting up rules for adding discovered devices to administration groups (optional)**

   New devices appear on the network as a result of being detected as part of network polls. These automatically fall into the **Unassigned devices** group. If you want, you can set up the rules for automatically moving these devices to the **Managed devices** group. You can also establish retention rules.

   If you skip this rule-setting stage, all the newly discovered devices go to the **Unassigned devices** group and stay there. If you want, you can move these devices to the **Managed devices** group manually. If you move the devices to the **Managed devices** group manually, you can analyze information about each device and decide whether you want to move it to an administration group, and, if so, to which group.

### Results

Completion of the scenario yields the following:

- Kaspersky Security Center Linux Administration Server discovers the devices that are on the network and provides you with information about them.
- Future polls are set up and are conducted according to the specified schedule.

Newly discovered devices are allocated in accordance with the specified rules. If no rules are configured, the devices stay in the **Unassigned devices** group.

# Windows network polling

### About Windows network polling

Kaspersky Security Center Linux Administration Server does not support Windows network polling. Use Windows-based distribution points to poll Windows networks.

During a quick poll, distribution points only retrieve information from the list of the NetBIOS names of devices in all network domains and workgroups. During a full poll, the following information is requested from each client device:

- Operating system name
- IP address
- DNS name
- NetBIOS name

Both quick polls and full polls require the following:

- Ports UDP 137/138, TCP 139, UDP 445, TCP 445 must be available in the network.
- The SMB protocol is enabled.
- The Microsoft Computer Browser service must be used, and the primary browser computer must be enabled on the Administration Server.
- The Microsoft Computer Browser service must be used, and the primary browser computer must be enabled on the client devices:
  - On at least one device, if the number of networked devices does not exceed 32.
  - On at least one device for each 32 networked devices.

The full poll can run only if the quick poll has run at least once.

# IP range polling

Kaspersky Security Center Linux attempts to perform reverse name resolution for every IPv4 address from the specified range to a DNS name using standard DNS requests. If this operation succeeds, the server sends an `ICMP ECHO REQUEST` (the same as the ping command) to the received name. If the device responds, the information about it is added to the Kaspersky Security Center Linux database. The reverse name resolution is necessary to exclude network devices that can have an IP address but are not computers, for example, network printers or routers.

This polling method relies upon a correctly configured local DNS service. It must have a reverse lookup zone. If this zone is not configured, IP subnet polling will yield no results.

Initially, Kaspersky Security Center Linux gets IP ranges for polling from the network settings of the device on which it is installed. If the device address is 192.168.0.1 and the subnet mask is 255.255.255.0, Kaspersky Security Center Linux includes the network 192.168.0.0/24 in the list of polling address automatically. Kaspersky Security Center Linux polls all addresses from 192.168.0.1 to 192.168.0.254.

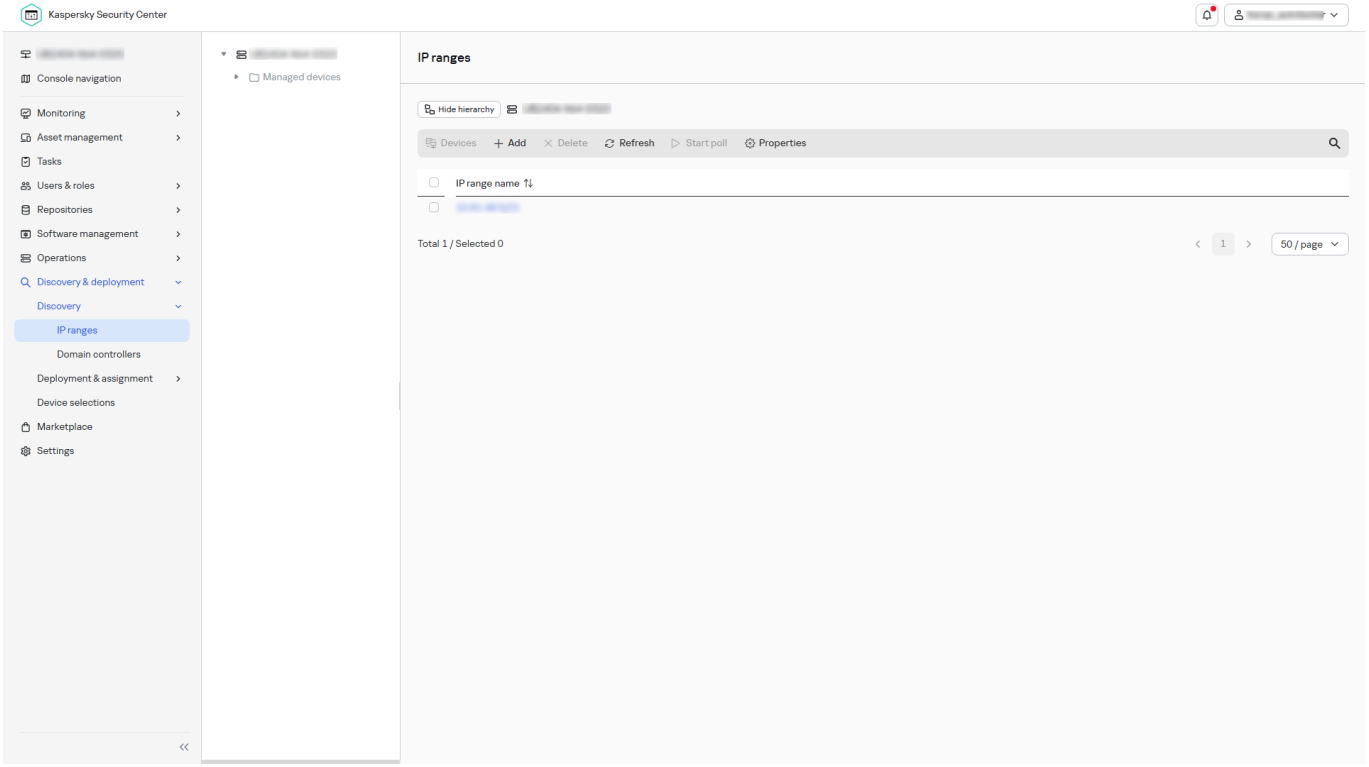
If only IP range polling is enabled, Kaspersky Security Center Linux discovers devices only with IPv4 addresses. If your network includes IPv6 devices, turn on Zeroconf polling of devices.

For all Linux-based hosts within a Microsoft Active Directory, Samba, FreeIPA, or ALD Pro domain controller, specify the `netbios name` and `workgroup` parameters in the `/etc/samba/smb.conf` file. Otherwise, polling results may contain duplicate hosts.

## Viewing and modifying the settings for IP range polling

*To view and modify the properties of IP range polling:*

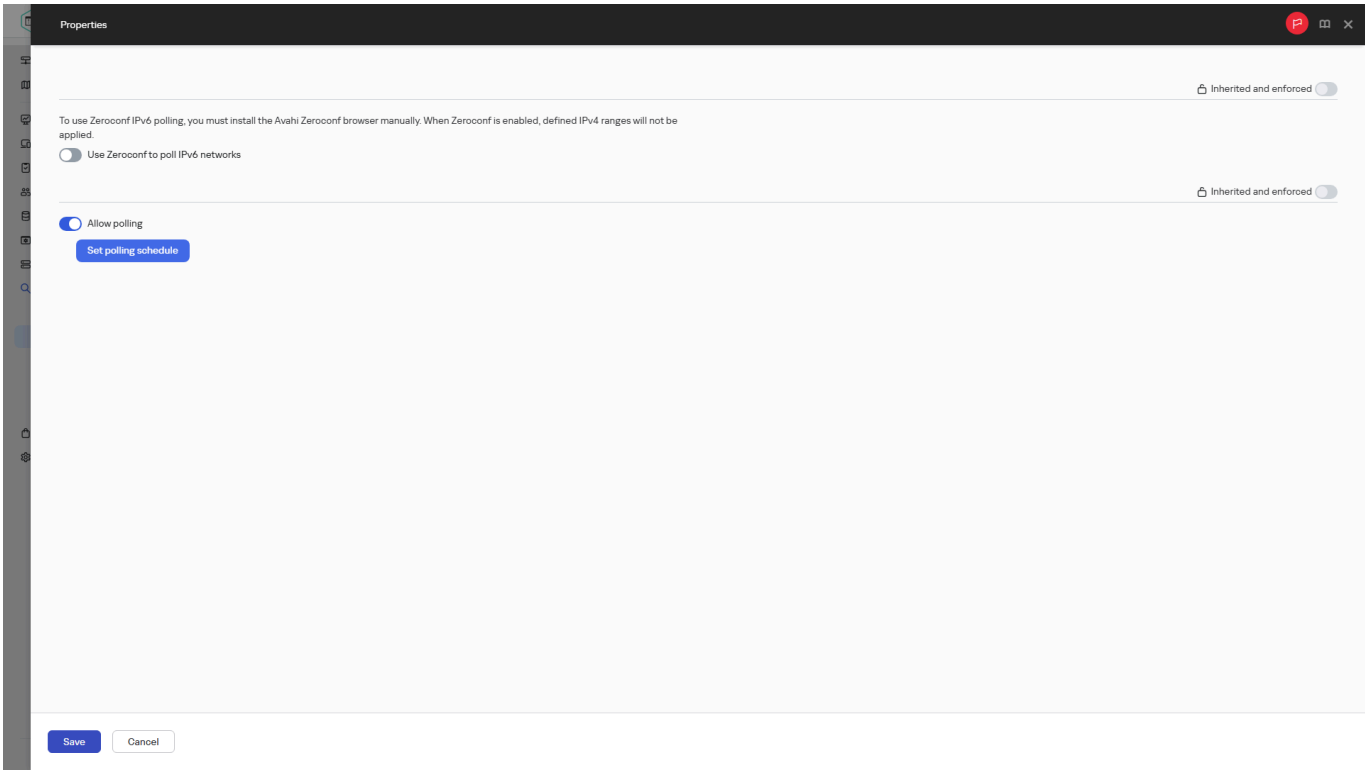
1. In the main menu, go to **Discovery & deployment** → **Discovery** → **IP ranges**.




IP range list

2. Click the **Properties** button.

   The IP polling properties window opens.




The IP polling properties

3. Enable or disable IP polling by using the **Allow polling** toggle button.

4. Configure the polling schedule. By default, IP polling runs every 420 minutes (seven hours).

   When specifying the polling interval, make sure that this setting does not exceed the value of the IP address lifetime parameter. If an IP address is not verified by polling during the IP address lifetime, this IP address is automatically removed from the polling results. By default, the life span of the polling results is 24 hours, because dynamic IP addresses (assigned using Dynamic Host Configuration Protocol (DHCP)) change every 24 hours.

   Polling schedule options:

   - **Every N days**

     The polling runs regularly, with the specified interval in days, starting from the specified date and time.

     By default, the polling runs every day, starting from the current system date and time.

   - **Every N minutes**

     The polling runs regularly, with the specified interval in minutes, starting from the specified time.

   - **By days of week**

     The polling runs regularly, on the specified days of week, and at the specified time.

   - **Monthly on selected weekday**

     The polling runs regularly, on the specified days of each month, and at the specified time.

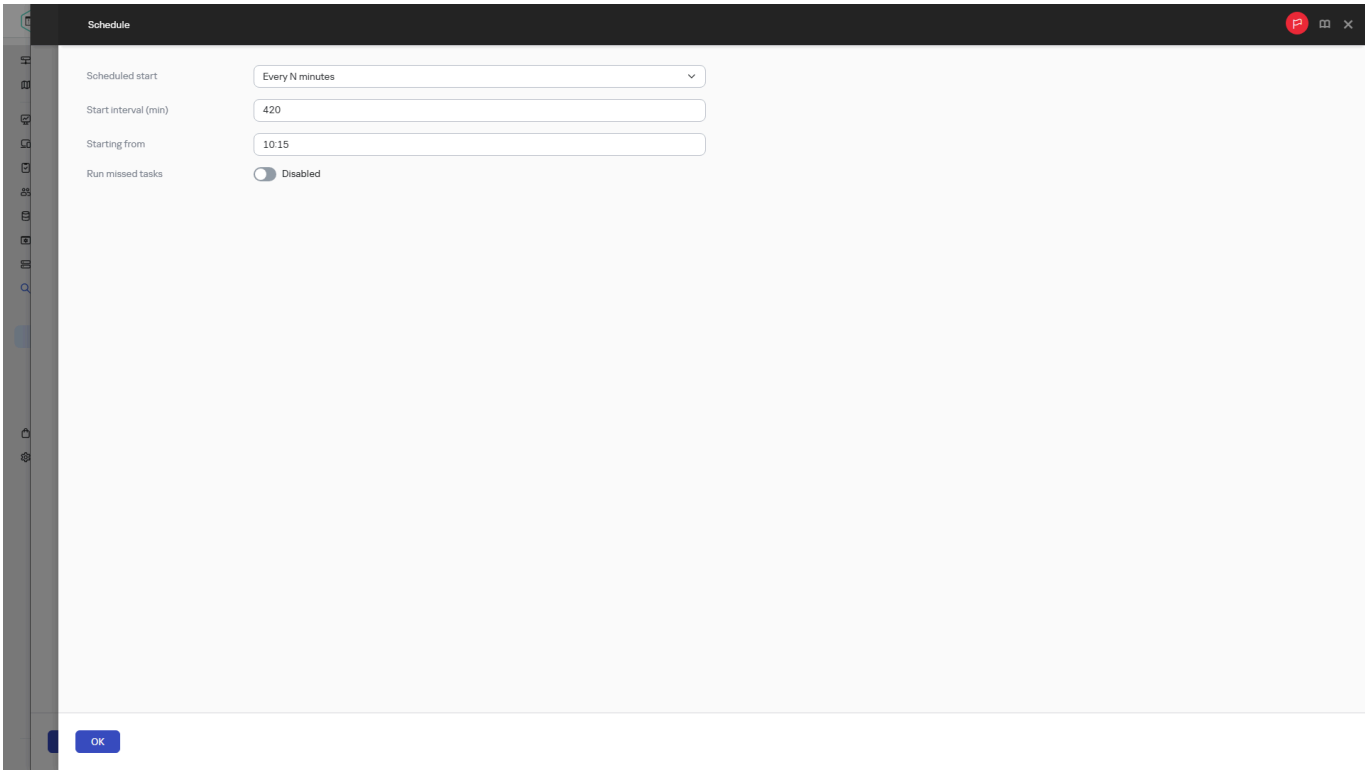
   - **Run missed tasks**

     If the Administration Server is switched off or unavailable during the time for which the poll is scheduled, the Administration Server can either start the poll immediately after it is switched on, or wait for the next time for which the poll scheduled.

     If this option is enabled, the Administration Server starts polling immediately after it is switched on.

     If this option is disabled, the Administration Server waits for the next time for which the polling is scheduled.

By default, this option is disabled.




Configuring the polling schedule

5. Click the **Save** button.

The properties are saved and applied to all IP ranges.

### Running the poll manually

*To run the poll immediately,*

Click **Start poll**.

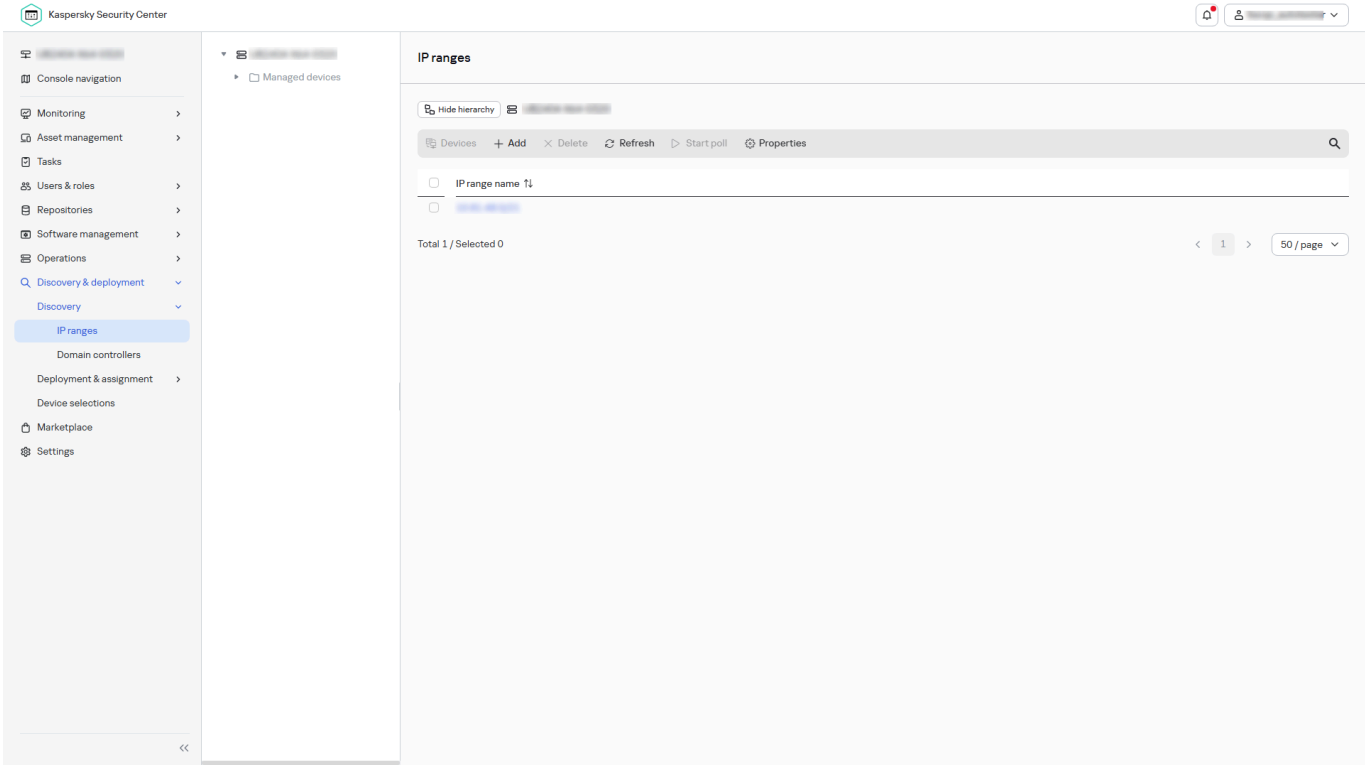
# Adding and modifying an IP range

Initially, Kaspersky Security Center Linux gets IP ranges for polling from the network settings of the device on which it is installed. If the device address is 192.168.0.1 and the subnet mask is 255.255.255.0, Kaspersky Security Center Linux includes the network 192.168.0.0/24 in the list of polling address automatically. Kaspersky Security Center Linux polls all addresses from 192.168.0.1 to 192.168.0.254. You can modify the automatically defined IP ranges or add custom IP ranges.

You can create a range only for IPv4 addresses. If you enable Zeroconf polling, Kaspersky Security Center Linux will poll the whole network.

*To add a new IP range:*

1. In the main menu, go to **Discovery & deployment → Discovery → IP ranges**.




IP range list

2. To add a new IP range, click the **Add** button.

3. In the window that opens, specify the following settings:

   **IP range name**

   A name of the IP range. You might want to specify the IP range itself as its name, for example, "192.168.0.0/24".

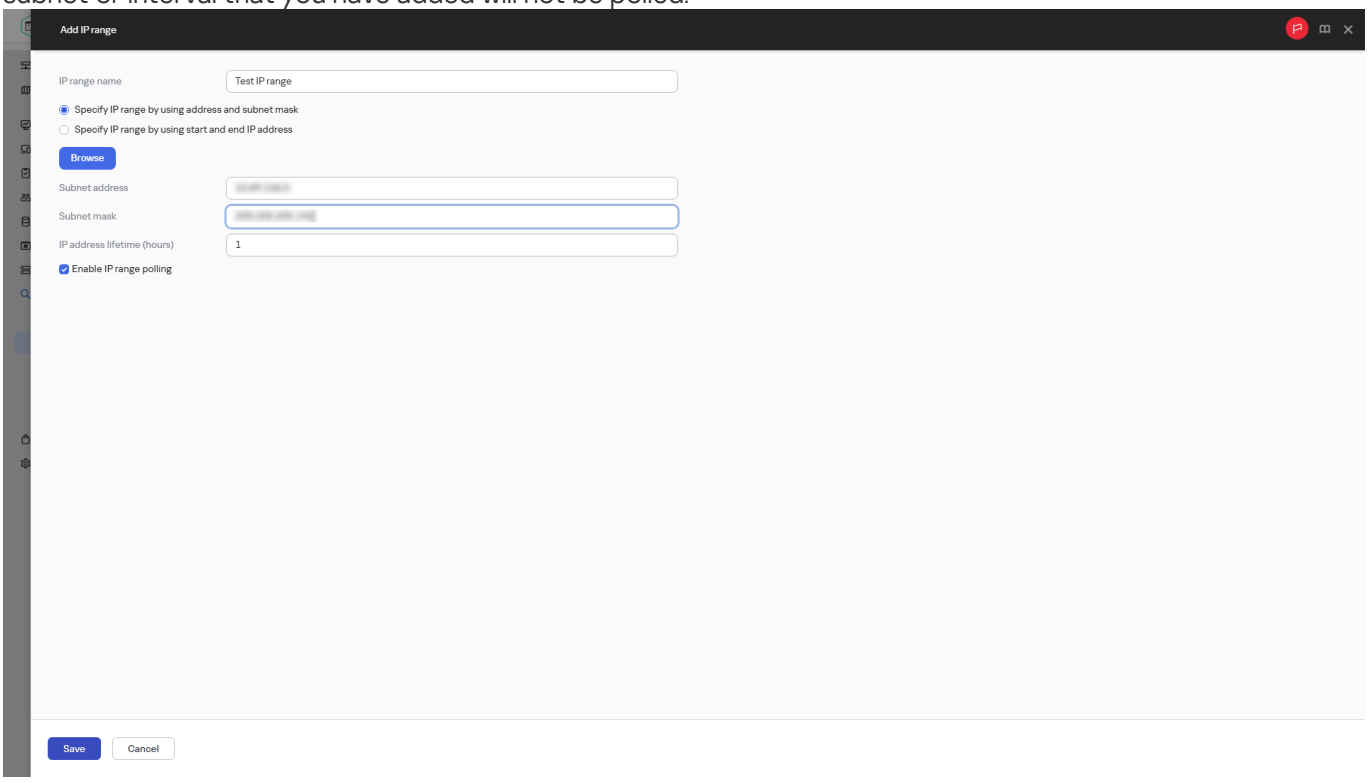
   **IP interval or subnet address and mask**

   Set the IP range by specifying either the start and end IP addresses or the subnet address and subnet mask. You can also select one of the already existing IP ranges by clicking the **Browse** button.

   **IP address lifetime (hours)**

   When specifying this parameter make sure that it exceeds the polling interval set in the polling schedule. If an IP address is not verified by polling during the IP address lifetime, this IP address is automatically removed from the polling results. By default, the life span of the polling results is 24 hours, because dynamic IP addresses (assigned using Dynamic Host Configuration Protocol (DHCP)) change every 24 hours.

4. Select **Enable IP range polling** if you want to poll the subnet or interval that you have added. Otherwise, the subnet or interval that you have added will not be polled.




Specifying IP range settings

5. Click the **Save** button.

   The new IP range is added to the list of IP ranges.

You can run polling of each IP range separately by using the **Start poll** button. By default, the life span of the polling results is 24 hours and it is equal to the IP address lifetime setting.

*To add a subnet to an existing IP range:*

1. In the main menu, go to **Discovery & deployment** → **Discovery** → **IP ranges**.
2. Click the name of the IP range to which you want to add a subnet.
3. In the window that opens, click the **Add** button.
4. Specify a subnet by using either its address and mask, or by using the first and last IP address in the IP range. Or, add an existing subnet by clicking the **Browse** button.
5. Click the **Save** button.

   The new subnet is added to the IP range.
6. Click the **Save** button.

The new settings of the IP range are saved.

You can add as many subnets as you need. Named IP ranges are not allowed to overlap, but unnamed subnets inside an IP range have no such restrictions. You can enable and disable polling independently for every IP range.

# Zeroconf polling

This polling type is supported only for Linux-based distribution points.

Kaspersky Security Center Linux can poll networks that have devices with IPv6 addresses. In this case, IP ranges are not specified and Kaspersky Security Center Linux polls the whole network by using zero-configuration networking (also referred to as *Zeroconf*). To start using Zeroconf, you must install avahi components (avahi-utils) on the Linux device that polls networks, that is, the Administration Server or a distribution point.

When using Zeroconf, the Administration Server or distribution point scans the network to discover devices that support the Zeroconf protocol and temporarily adds such devices to the list. An ICMPv6 ping is then performed for each device to verify availability, and then the avahi service does a reverse DNS lookup to resolve the IPv6 addresses to DNS names. Information about the host system (DNS name and OS type) is registered in the Kaspersky Security Center Linux database.

The scope of the Zeroconf poll is determined by the settings of the avahi service. By default, a broadcast poll is made within one subnet. If multiple network interfaces are configured on the device hosting the Administration Server or distribution point, the avahi service polls the subnets associated with all active interfaces.

## Recommendations for successful completion of a Zeroconf poll

- Make sure that the following settings have been made in the /etc/avahi/avahi-daemon.conf file:
  - On the Administration Server or distribution point:
    `[server]`
    `use-ipv6=yes`
  - On devices:
    `[server]`
    `use-ipv6=yes`
    `[publish]`
    `publish-addresses=yes`
    `publish-workstation=yes`
- Make sure that the following line is present in the /etc/nsswitch.conf file:
  - On the Administration Server or distribution point:
    `mdns_minimal [NOTFOUND=return] dns`

*To enable Zeroconf polling:*

1. In the main menu, go to **Discovery & deployment** → **Discovery** → **IP ranges**.
2. Click the **Properties** button.

3. In the opened window, turn on the **Use Zeroconf to poll IPv6 networks** toggle button.

After that, Kaspersky Security Center Linux starts to poll your network. In this case, the specified IP ranges are ignored.

# Domain controller polling

Kaspersky Security Center Linux supports polling of the following domain controller types:

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

For a Samba domain controller, Samba 4 is used as an Active Directory domain controller.

When you poll a domain controller, Administration Server or a distribution point retrieves information about the domain structure, user accounts, security groups, and DNS names of the devices that are included in the domain.

We recommend using domain controller polling if all networked devices are members of a domain. If some of the networked devices are not included in the domain, these devices cannot be discovered by domain controller polling.

## Prerequisites

Before you poll a domain controller, ensure that you allow connections to the domain controller through a firewall or a proxy server. Also ensure that the following protocols are enabled on the domain controller:

- Lightweight Directory Access Protocol (LDAP)
- Simple Authentication and Security Layer (SASL)

  This protocol is used if connection to the domain controller is established by using the SASL authentication. Administration Server and distribution points supports only the DIGEST-MD5 mechanism.
- Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS)

  This protocol is used if you need to connect to the domain controller over an encrypted connection.

Ensure that the following ports are available on the domain controller device:

- 389 for the LDAP protocol and Simple Authentication (including SASL)
- 636 for the LDAPS protocol

For FreeIPA and ALD Pro, the LDAP and LDAPS protocols are used only for domain polling. Kaspersky Security Center Linux does not support authentication of FreeIPA accounts via LDAP(S). To allow FreeIPA and ALD Pro users to log in to Web Console, you must configure Kerberos authentication via the IAM service.

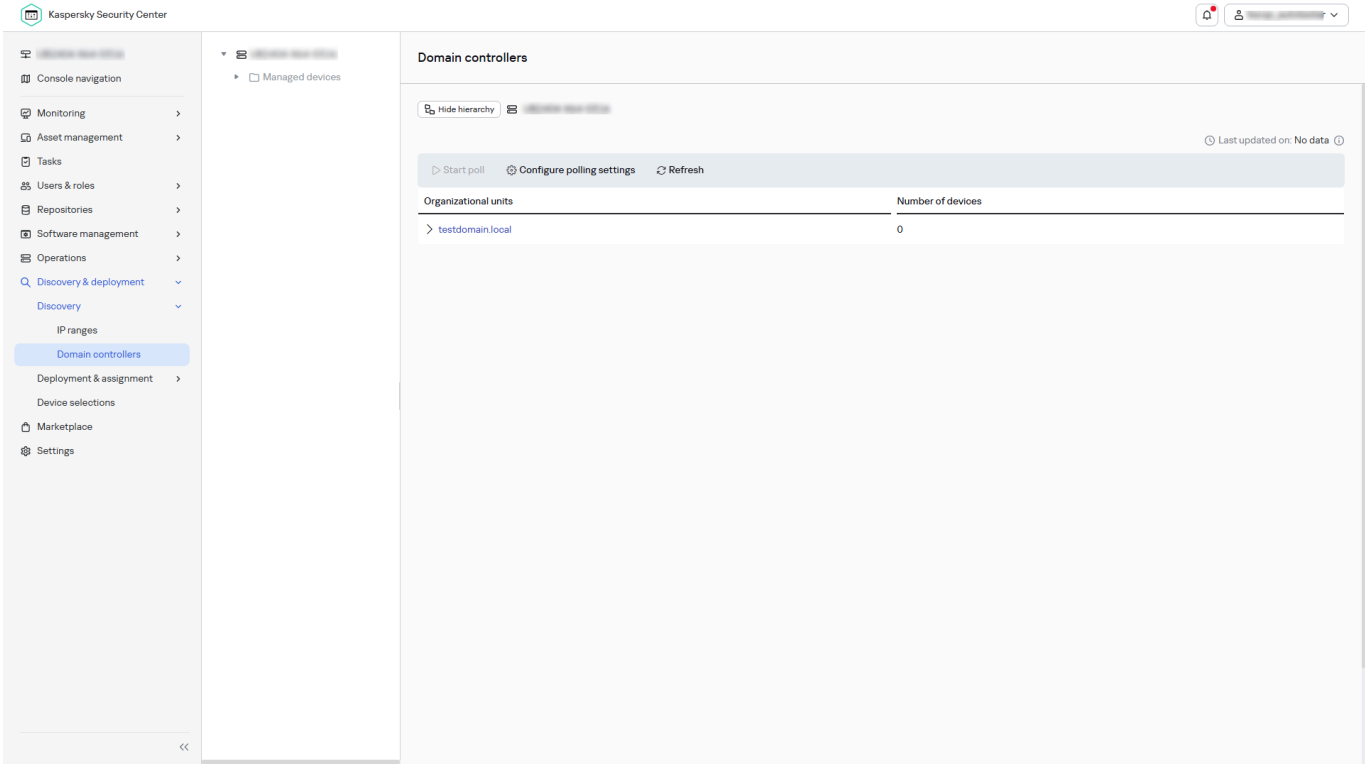
For all Linux-based hosts within a Microsoft Active Directory, Samba, FreeIPA, or ALD Pro domain controller, you need to specify the `netbios name` and `workgroup` parameters in the `/etc/samba/smb.conf` file. Otherwise, polling results may contain duplicate hosts.

If a Microsoft Active Directory domain contains multiple domain controllers, selecting a specific controller during domain polling is not supported. The connection is established with the first detected domain controller. To ensure proper authentication with the Microsoft Active Directory domain, the Subject Alternative Name (SAN) field of the certificate must include all addresses of the domain controllers included in this domain, as well as the NetBIOS name of the Microsoft Active Directory domain.

## Domain controller polling by using Administration Server

*To poll a domain controller by using Administration Server:*

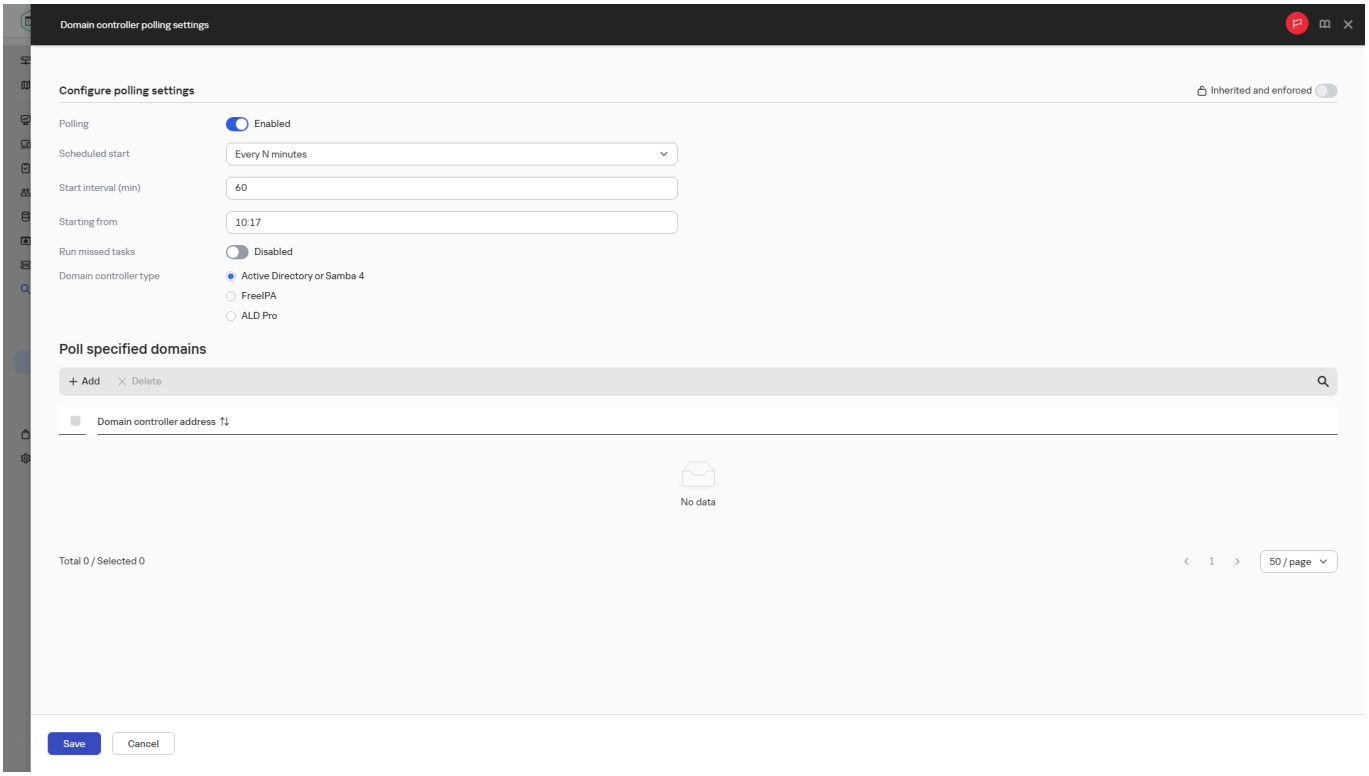
1. In the main menu, go to **Discovery & deployment** → **Discovery** → **Domain controllers**.




Domain controller polling window

2. Click **Configure polling settings**.

The **Domain controller polling settings** window opens.




Domain controller polling settings

3. In the **Polling** field, switch the toggle button to the **Enabled** position.

4. In the **Poll specified domains**, click **Add**, and then specify the address and user credentials of the domain controller.

5. In the **Domain controller polling settings** window, do the following:

   - Select the type of the domain controller to be polled: **Active Directory or Samba 4**, **FreeIPA**, **ALD Pro**.

   - If necessary, set the polling schedule. The default period is one hour. The data received at the next polling completely replaces old data.

     The following polling schedule options are available:

     **Every N days**

     The polling runs regularly, with the specified interval in days, starting from the specified date and time.

     By default, the polling runs every day, starting from the current system date and time.

     **Every N minutes**

     The polling runs regularly, with the specified interval in minutes, starting from the specified time.

     **By days of week**

     The polling runs regularly, on the specified days of week, and at the specified time.

     **Monthly on selected weekday**

     The polling runs regularly, on the specified days of each month, and at the specified time.

     **Run missed tasks**

If the Administration Server is switched off or unavailable during the time for which the poll is scheduled, the Administration Server can either start the poll immediately after it is switched on, or wait for the next time for which the poll scheduled.

If this option is enabled, the Administration Server starts polling immediately after it is switched on.

If this option is disabled, the Administration Server waits for the next time for which the polling is scheduled.

By default, this option is disabled.

If you change user accounts in a security group of the domain, these changes will be displayed in Kaspersky Security Center Linux an hour after you poll the domain controller.

6. Click **Save** to apply changes.
7. If you want to perform the poll immediately, click the **Start poll** button.

## Domain controller polling by using a distribution point

You can also poll a domain controller by using a distribution point. A Windows- or Linux-based managed device can act as a distribution point.

For a Linux distribution point, polling of all domain controller types is supported.
For a Windows distribution point, only polling of a Microsoft Active Directory domain controller is supported.
Polling with a Mac distribution point is not supported.

*To configure domain controller polling by using the distribution point:*

1. Open the distribution point properties.
2. Select the **Domain controller polling** section.
3. In the **Polling** field, switch the toggle button to the **Enabled** position.
4. If you use a Linux distribution point, select the type of the domain controller to be polled: **Active Directory or Samba 4**, **FreeIPA**, **ALD Pro**.

   This is not necessary that you specify the same domain controller type when configuring polling by using a distribution point and by using Administration Server.
5. Select the domain controller that you want to poll.

   If you use a Linux distribution point, in the **Poll specified domains** section, click **Add**, and then specify the address and user credentials of the domain controller.

   If you use a Windows distribution point, you can select one of the following options:

   - **Poll current domain**
   - **Poll entire domain forest**
   - **Poll specified domains**

6. Click the **Set polling schedule** button to specify the polling schedule options, if needed.

   Polling starts only according to the specified schedule. A manual start of polling is not available.

After the polling is completed, the domain structure will be displayed in the **Domain controllers** section.

If you set up and enabled device moving rules, the newly discovered devices are automatically included in the **Managed devices** group. If no moving rules have been enabled, the newly discovered devices are automatically included in the **Unassigned devices** group.

The discovered user accounts can be used for domain authentication in Kaspersky Security Center Web Console.

# Authentication and connection to a domain controller

## Authentication and connection to a domain controller when polling a domain

When polling a domain controller, Administration Server or a distribution point identifies the connection protocol to establish initial connection to the domain controller. This protocol is used for all future connections to the domain controller. When establishing the initial connection to the domain controller, you can change connection options by using the Network Agent flags (`KLNAG_LDAP_TLS_REQCERT` and `KLNAG_LDAP_SSL_CACERT`). You can configure the Network Agent flags by using klscflag as described in this article.

The initial connection to a domain controller proceeds as follows:

1. Administration Server or a distribution point attempts to connect to the domain controller over LDAPS.

   By default, certificate verification is not required. Set the `KLNAG_LDAP_TLS_REQCERT` flag to 1 to enforce certificate verification.

   Possible values of the `KLNAG_LDAP_TLS_REQCERT` flag:

   - `0`—The certificate is requested, but if it is not provided or the certificate verification failed, then the TLS connection is still considered successfully created (default value).
   - `1`—Strict verification of the LDAP server certificate is required.

   By default, when the `KLNAG_LDAP_SSL_CACERT` flag is not specified, the OS-dependent path to the certificate authority (CA) is used to access the certificate chain. Use the `KLNAG_LDAP_SSL_CACERT` flag to specify a custom path.

2. If the LDAPS connection fails, Administration Server or a distribution point attempts to connect to the domain controller over non-encrypted TCP connection by using SASL (DIGEST-MD5).

### Authentication and connection to a domain controller when authenticating a domain user to Administration Server

When a domain user authenticates on Administration Server, Administration Server identifies the protocol to establish connection to the domain controller.

For FreeIPA and ALD Pro, the LDAP and LDAPS protocols are used only for domain polling. Kaspersky Security Center Linux does not support authentication of FreeIPA accounts via LDAP(S). To allow FreeIPA and ALD Pro users to log in to Web Console, you must configure Kerberos authentication via the IAM service.

The connection to a domain controller proceeds as follows:

1. Administration Server attempts to connect to the domain controller over LDAPS.

   Strict verification of the LDAP server certificate is required.

   By default, when the `KLNAG_LDAP_SSL_CACERT` flag is not specified, the OS-dependent path to the certificate authority (CA) is used to access the certificate chain. Use the `KLNAG_LDAP_SSL_CACERT` flag to specify a custom path.

2. If the LDAPS connection fails, an error connecting to the domain controller occurs and other connection protocols are not used.

### Configuring flags

You can use the klscflag utility to configure flags.

Run the command line, and then change your current directory to the directory with the klscflag utility. On the Administration Server device, the klscflag utility is located in the installation directory. The default installation path is /opt/kaspersky/ksc64/sbin.

For example, the following command enforces certificate verification:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

# Configuring domain authentication for the Administration Server using flags

Only Simple/SASL authentication (with a password; SASL DIGEST-MD5; SASL EXTERNAL-TLS) is supported on an Administration Server via Microsoft Active Directory.

FreeIPA/ALD Pro authentication is not supported.

*To perform Simple/SASL domain authentication:*

1. Configure LDAPS (LDAP over TLS) on the domain controller.

   To do this, on the domain controller, obtain, install, and configure a root and/or intermediate certificate of the certification authority that issued the certificate to the controller, or a self-signed certificate of the domain controller. The procedure for configuring a certificate for LDAPS is described in the Microsoft Active Directory documentation.

2. In the **SAN** field of the certificate, specify the addresses of all domain controllers and the domain name.

   During authentication, the Administration Server will perform a strict validation of the domain controller certificate.

3. Place the domain controller certificate in the system certificate store.

   If you want to store the certificate in a separate directory, specify the path to the LDAP server certificate file using the KLNAG_LDAP_SSL_CACERT flag:

   ```
   klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v
   "/var/opt/kaspersky/ldap_cert.crt"
   ```

The domain scan is completed.

**Click here** to view examples of installing a domain controller certificate in the system certificate store for various operating systems.

**For Ubuntu/Debian operating systems**

1. If you do not have the package for managing the system certificate store installed, install it by running the following command:

   ```
   sudo apt-get install -y ca-certificates
   ```

2. Copy the certificate file to the /usr/local/share/ca-certificates directory by running the following command:

   ```
   sudo cp local-ca.crt /usr/local/share/ca-certificates
   ```

   where `local-ca.crt` is an example certificate file name.

3. Add the certificate to the system store by running the following command:

   ```
   sudo cp local-ca.crt /usr/local/share/ca-certificates
   ```

**For CentOS operating system**

1. If you do not have the package for managing the system certificate store installed, install it by running the following command:

   ```
   sudo yum install -y ca-certificates
   ```

2. If you are using CentOS 7 or an earlier version, run the following command:

   ```
   sudo update-ca-trust force-enable
   ```

3. Copy the certificate file to the /etc/pki/ca-trust/source/anchors directory by running the following command:

   ```
   sudo cp local-ca.crt /etc/pki/ca-trust/source/anchors/
   ```

   where `local-ca.crt` is an example certificate file name.

4. Add the certificate to the system store by running the following command:

   ```
   sudo update-ca-trust
   ```

To configure Simple/SASL domain authentication, use the following flags:

- `KLNAG_LDAP_REFERRAL_BEHAVIOR` controls the processing of the referral response when searching for a user on the domain controller used for authentication.

  The default value is `KLNAG_LDAP_REFERRAL_BEHAVIOR = 1`

- `KLNAG_LDAP_USR_INFO_IGNORE_REF_ERR` controls the processing of a referral when requesting additional data for this user.

  The default value is `KLNAG_LDAP_USR_INFO_IGNORE_REF_ERR = 0`

We recommend keeping the default values of the flags, except in the following cases:

- Your infrastructure has multiple domain controllers and/or multiple domain zones, and the account used for authentication on the Administration Server can be located on different domain controllers with a different SID. At the same time, LDAP referrals from the global directory never lead to inaccessible controllers.

  Set `KLNAG_LDAP_REFERRAL_BEHAVIOR` to `2` by running the following command:

  ```
  ./klscflag -fset -pv klnagent -n KLNAG_LDAP_REFERRAL_BEHAVIOR -t d -v 2
  ```

- In your infrastructure, referrals pointing to unavailable domain controllers are possible (for example, due to network restrictions).

  Set `KLNAG_LDAP_REFERRAL_BEHAVIOR=0` and `KLNAG_LDAP_USR_INFO_IGNORE_REF_ERR=1` by running the following commands:

  ```
  ./klscflag -fset -pv klnagent -n KLNAG_LDAP_REFERRAL_BEHAVIOR -t d -v 0
  ./klscflag -fset -pv klnagent -n KLNAG_LDAP_USR_INFO_IGNORE_REF_ERR -t d -v 1
  ```

# Configuring a Samba domain controller

Kaspersky Security Center Linux supports a Linux domain controller running only on Samba 4.

A Samba domain controller supports the same schema extensions as a Microsoft Active Directory domain controller. You can enable full compatibility of a Samba domain controller with a Microsoft Active Directory domain controller by using the Samba 4 schema extension. This is an optional action.

> We recommend enabling full compatibility of a Samba domain controller with a Microsoft Active Directory domain controller. This will ensure the correct interaction between Kaspersky Security Center Linux and the Samba domain controller.

*To enable full compatibility of a Samba domain controller with a Microsoft Active Directory domain controller:*

1. Execute the following command to use the RFC2307 schema extension:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Enable the schema update in a Samba domain controller. To do this, add the following line to the `/etc/samba/smb.conf` file:

   ```
   dsdb:schema update allowed = true
   ```

If the schema update completes with an error, you need to perform a full restore of the domain controller that acts as a schema master.

For all Linux-based hosts within a Samba domain controller, specify the `netbios name` and `workgroup` parameters in the `/etc/samba/smb.conf` file. Otherwise, polling results may contain duplicate hosts.

# Equipment inventory

The hardware list (**Asset management** → **Hardware**) that you use to inventory equipment is populated in two ways: automatically and manually. After each network polling, all detected devices are added to the list automatically; however, you can also add devices manually if you do not want to poll the network. You can add other devices to the list manually, for example, routers, printers, or device hardware.

In the properties of a device, you can view and edit detailed information about that device.

The hardware list may contain the following types of devices:

- Computers
- Mobile devices
- Network devices
- Virtual devices
- OEM components
- Computer peripherals
- Connected devices
- VoIP phones
- Network repositories

The administrator can assign the *Enterprise equipment* attribute to detected devices. This attribute can be assigned manually in the properties of a device, or the administrator can specify criteria for the attribute to be assigned automatically. In this case, the *Enterprise equipment* attribute is assigned by device type.

Kaspersky Security Center Linux allows writing off equipment. To do this, select the **Written off** option in the properties of a device. The device is not displayed on the equipment list.

An administrator can manage the list of programmable logic controllers (PLC) in the **Hardware** folder. Detailed information on managing the PLC list is provided in the *Kaspersky Industrial CyberSecurity for Nodes User Guide*.

# Adding information about new devices

*To add information about new devices on the network:*

1. In the main menu, go to **Asset management** → **Hardware**.
2. Click the **Add** button to open the **New device** window.
3. In the **New device** window, in the **Device type** drop-down list select a device type that you want to add.
4. Click **OK**.

   The device properties window opens on the **General** section.
5. In the **General** section, fill in the entry fields with data on the device. The **General** section lists the following settings:

   - **Enterprise device**. Select the check box if you want to assign the *Enterprise* attribute to the device. Using this attribute, you can search for devices in the **Hardware** folder.
   - **Written off**. Select the check box if you do not want the device to be displayed in the list of devices in the **Hardware** folder.
6. Click **Apply**.

The new device will be displayed in the workspace of the **Hardware** page.

# Configuring criteria used to define enterprise devices

*To configure criteria of detection for enterprise devices:*

1. In the main menu, go to **Asset management** → **Hardware**.
2. At the top of the **Hardware** page, click the **Set up rule for Enterprise devices** link.

   A **Set up rule for Enterprise devices** panel is invoked.
3. In the **Set up rule for Enterprise devices** panel, enable the **Set the Enterprise device attribute automatically for the device**. Specify device types to which the *Enterprise* attribute is assigned automatically.

   This option affects only the devices that were added through network polling. For the devices added manually, set the *Enterprise* attribute manually.
4. Click **OK**.

The criteria of detection for enterprise devices are configured.

# Using VDI dynamic mode on client devices

A virtual infrastructure can be deployed on a corporate network using temporary virtual machines. Kaspersky Security Center Linux detects temporary virtual machines and adds information about them to the Administration Server database. After a user finishes using a temporary virtual machine, the machine is removed from the virtual infrastructure. However, a record about the removed virtual machine can be saved in the database of the Administration Server. Also, nonexistent virtual machines can be displayed in Kaspersky Security Center Web Console.

To prevent information about nonexistent virtual machines from being saved, Kaspersky Security Center Linux supports dynamic mode for Virtual Desktop Infrastructure (VDI). The administrator can enable support of dynamic mode for VDI in the properties of the installation package of Network Agent to be installed on the temporary virtual machine.

When a temporary virtual machine is disabled, Network Agent notifies the Administration Server that the machine has been disabled. If the virtual machine has been disabled successfully, it is removed from the list of devices connected to the Administration Server. If the virtual machine is disabled with errors and Network Agent does not send a notification about the disabled virtual machine to the Administration Server, a backup scenario is used. In this scenario, the virtual machine is removed from the list of devices connected to the Administration Server after three unsuccessful attempts to synchronize with the Administration Server.

# Enabling VDI dynamic mode in the properties of an installation package for Network Agent

*To enable VDI dynamic mode:*

1. In the main menu, go to **Software management** → **Installation packages**.
2. In the context menu of the Network Agent installation package, select **Properties**.

   The **Properties** window opens.
3. In the **Properties** window, select the **Advanced** section.
4. In the **Advanced** section, select the **Enable dynamic mode for VDI** option.

The device on which Network Agent is to be installed becomes a part of VDI.

# Moving devices from VDI to an administration group

*To move devices that are part of VDI to an administration group:*

1. Go to **Asset management** → **Moving rules**.
2. Click **Add**.
3. On the **Rule conditions** tab, select the **Virtual machines** tab.

4. Set the **This is a virtual machine** rule to **Yes** and **Part of Virtual Desktop Infrastructure** to **Yes.**

5. Click **Save**.

# Managing client devices

Kaspersky Security Center Linux allows you to manage client devices:

- View settings and statuses of managed devices, including clusters and server arrays.
- Configure distribution points.
- Manage tasks.

You can use administration groups to combine client devices in a set that can be managed as a single unit. A client device can be included in only one administration group. Devices can be allocated to a group automatically based on **Rule conditions**:

- Creating device moving rules.
- Copying device moving rules.
- Conditions for a device moving rule.

You can use device selections to filter devices based on a condition. You can also tag devices for creating selections, for finding devices, and for distributing devices among administration groups.

# Settings of a managed device

*To view the settings of a managed device:*

1. In the main menu, go to **Asset management** → **Managed devices**.

   The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the required device.

The properties window of the selected device is displayed.

The following tabs are displayed in the upper part of the properties window representing the main groups of the settings:

**General**

This tab comprises the following sections:

- The **General** section displays general information about the client device. Information is provided on the basis of data received during the last synchronization of the client device with the Administration Server:

  - **Name**

    In this field, you can view and modify the client device name in the administration group.

  - **Description**

    In this field, you can enter an additional description for the client device.

- **Device status**

  Status of the client device assigned on the basis of the criteria defined by the administrator for the status of anti-virus protection on the device and the activity of the device on the network.

- **Full group name**

  Administration group, which includes the client device.

- **Last update of anti-virus databases**

  Date the anti-virus databases or applications were last updated on the device.

- **Connected to Administration Server**

  Date and time Network Agent installed on the client device last connected to the Administration Server.

- **Last visible**

  Date and time the device was last visible on the network.

- **Network Agent version**

  Version of the installed Network Agent.

- **Created**

  Date of the device creation within Kaspersky Security Center Linux.

- **Device owner**

  Name of the device owner. You can assign or remove a user as a device owner by clicking the **Manage device owner** link.

- **Do not disconnect from the Administration Server**

  If this option is enabled, continuous connectivity between the managed device and the Administration Server is maintained. You may want to use this option if you are not using push servers, which provide such connectivity.

  If this option is disabled and push servers are not in use, the managed device only connects to the Administration Server to synchronize data or to transmit information.

  The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

  This option is disabled by default on managed devices. This option is enabled by default on the device where the Administration Server is installed and stays enabled even if you try to disable it.

- The **Network** section displays the following information about the network properties of the client device:

  - **IP address**

    Device IP address.

  - **Windows domain**

    Workgroup that contains the device.

  - **DNS name**

DNS domain name of the client device.

- **NetBIOS name**

  Name of the client device.

- **IPv6 address**

- The **System** section provides information about the operating system installed on the client device:
  - **OS**
  - **CPU architecture**
  - **Device name**
  - **Virtual machine type**

    The virtual machine manufacturer.

  - **Dynamic virtual machine as part of VDI**

    This row displays whether the client device is a dynamic virtual machine as part of VDI.

- The **Protection** section provides the following information about the current status of anti-virus protection on the client device:
  - **Visible**

    Visibility status of the client device.

  - **Device status**

    Status of the client device assigned on the basis of the criteria defined by the administrator for the status of anti-virus protection on the device and the activity of the device on the network.

  - **Status description**

    Status of the client device protection and connection to Administration Server.

  - **Protection status**

    This field shows the current status of real-time protection on the client device.

    When the status changes on the device, the new status is displayed in the device properties window only after the client device is synchronized with the Administration Server.

  - **Last full scan**

    Date and time the last malware scan was performed on the client device.

  - **Virus detected**

    Total number of threats detected on the client device since installation of the security application (first scan), or since the last reset of the threat counter.

  - **Objects that have failed disinfection**

    Number of unprocessed files on the client device.

This field ignores the number of unprocessed files on mobile devices.

- **Disk encryption status**

  The current status of file encryption on the local drives of the device. For a description of the statuses, see the Kaspersky Endpoint Security for Windows Help.

  Files can be only encrypted on the managed devices on which Kaspersky Endpoint Security for Windows is installed.

- The **Device status defined by application** section provides information about the device status that is defined by the managed application installed on the device. This device status can differ from the one defined by Kaspersky Security Center Linux.

**Applications**

This tab lists all Kaspersky applications installed on the client device. This tab contains the **Start** and **Stop** buttons that start and stop the selected Kaspersky application (except for Network Agent). You can use these buttons if port 15000 UDP is available on the managed device for receipt push-notifications from Administration Server. If the managed device is unavailable for push-notifications, but the mode of continuous connection to Administration Server is enabled (the **Do not disconnect from the Administration Server** option in the **General** section is enabled), the **Start** and **Stop** buttons are available too. Otherwise, when you try to start or stop the application, an error message is displayed. Also you can click the application name to view general information about the application, a list of events that have occurred on the device, and the application settings.

**Active policies and policy profiles**

This tab lists the policies and policy profiles that are currently assigned to the managed device.

**Tasks**

On the **Tasks** tab, you can manage client device tasks: view the list of existing tasks, create new ones, remove, start and stop tasks, modify their settings, and view execution results. The list of tasks is provided based on data received during the last session of client synchronization with the Administration Server. The Administration Server requests the task status details from the client device. If port 15000 UDP is available on the managed device for receipt push-notifications from Administration Server, the task status is displayed and buttons for managing the task are enabled. If a push server cannot reach the managed device, but the mode of continuous connection to Administration Server is enabled (the **Do not disconnect from the Administration Server** option in the **General** section is enabled), the actions with tasks are available too.

If connection is not established, the status is not displayed and buttons are disabled.

**Events**

The **Events** tab displays events logged on the Administration Server for the selected client device.

You can export, copy, and delete the device events.

**Security issues**

In the **Security issues** tab, you can view, edit, and create security issues for the client device. Security issues can be created either automatically, through managed Kaspersky applications installed on the client device, or manually by the administrator. For example, if some users regularly move malware from their removable drives to devices, the administrator can create a security issue. The administrator can provide a brief description of the case and recommended actions (such as disciplinary actions to be taken against a user) in the text of the security issue, and can add a link to the user or users.

A security issue for which all of the required actions have been taken is called *processed*. The presence of unprocessed security issues can be chosen as the condition for a change of the device status to *Critical* or *Warning*.

This section contains a list of security issues that have been created for the device. Security issues are classified by severity level and type. The type of a security issue is defined by the Kaspersky application, which creates the security issue. You can highlight processed security issues in the list by selecting the check box in the **Processed** column.

**Tags**

In the **Tags** tab, you can manage the list of keywords that are used for finding client devices: view the list of existing tags, assign tags from the list, configure auto-tagging rules, add new tags and rename old tags, and remove tags.

**Advanced**

This tab comprises the following sections:

- **Applications registry**. In this section, you can view the registry of applications installed on the client device and their updates; you can also set up the display of the applications registry.

  Information about installed applications is provided if Network Agent installed on the client device sends required information to the Administration Server. You can configure sending of information to the Administration Server in the properties window of Network Agent or its policy, in the **Repositories** section.

  Clicking an application name opens a window that contains the application details and a list of the update packages installed for the application.

- **Executable files**. This section displays executable files found on the client device.

- **Distribution points**. This section provides a list of distribution points with which the device interacts.

  - **Export to file**

    Click the **Export to file** button to save to a file a list of distribution points with which the device interacts. By default, the application exports the list of devices to a CSV file.

  - **Properties**

    Click the **Properties** button to view and configure the distribution point with which the device interacts.

- **Hardware registry**. In this section, you can view information about hardware installed on the client device.

  If Network Agent is installed on a device running Windows, it sends to the Administration Server the following information about the device hardware:

  - RAM
  - Mass storage devices
  - Motherboard
  - CPU
  - Network adapters
  - Monitors
  - Video adapter
  - Sound card

If Network Agent is installed on a device running Linux or macOS, it sends to the Administration Server the following information about the device hardware, if this information is provided by the operating system:

- Total RAM volume
- Total volume of mass storage devices
- Motherboard
- CPU
- Network adapters

- **Available updates**. This section displays a list of software updates found on this device but not installed yet.
- **Software vulnerabilities**. This section provides information about vulnerabilities in third-party applications installed on client devices.

  To save the vulnerabilities to a file, select the check boxes next to the vulnerabilities that you want to save, and then click the **Export to CSV** button or **Export to TXT** button.

  The section contains the following settings:

  - **Show only vulnerabilities that can be fixed**

    If this option is enabled, the section displays vulnerabilities that can be fixed by using a patch.

    If this option is disabled, the section displays both vulnerabilities that can be fixed by using a patch, and vulnerabilities for which no patch has been released.

    By default, this option is enabled.

  - **Vulnerability properties**

    Click a software vulnerability name in the list to view the properties of the selected software vulnerability in a separate window. In the window, you can do the following:

    - Ignore software vulnerability on this managed device (in Kaspersky Security Center Web Console).
    - View the list of recommended fixes for the vulnerability.
    - Manually specify the software updates to fix the vulnerability (in Kaspersky Security Center Web Console).
    - View vulnerability instances.
    - View the list of existing tasks to fix vulnerability and create new tasks to fix vulnerability.

- **Remote diagnostics**. In this section, you can perform remote diagnostics of client devices.

If you use a PostgreSQL, MariaDB or MySQL DBMS, the **Events** tab may display an incomplete list of events for the selected client device. This occurs when the DBMS stores a very large amount of events. You can increase the number of displayed events by doing either of the following:

- Removing unnecessary events.
- Reducing the storage term for unnecessary events.

To see a full list of events logged on the Administration Server for the device, use Reports.

# Manually checking the connection between a client device and the Administration Server. klnagchk utility

You can check the connection, and obtain detailed information about the settings of the connection, between a client device and Administration Server by using the klnagchk utility. The klnagchk utility is located in the Network Agent installation folder.

When started from the command line, the klnagchk utility can perform the following actions (depending on the keys in use):

- Display on the screen or logs the values of the settings used for connecting Network Agent installed on the device to Administration Server.
- Record into an event log file Network Agent statistics (since its last startup) and utility operation results, or displays the information on the screen.
- Attempt to establish a connection between Network Agent and Administration Server.

  If the connection attempt fails, the utility sends an ICMP packet to check the status of the device on which Administration Server is installed.

*To check the connection between a client device and Administration Server by using the klnagchk utility,*

On the device with Network Agent installed, start the klnagchk utility from the command line under a local administrator account.

Utility command line syntax:

```
klnagchk [-logfile <file name>] [-sp] [-savecert <path to certificate file>] [-
restart][-sendhb]
```

Descriptions of the keys:

- `-logfile <file name>`—Records in a log file with the values of the connection settings between Network Agent and Administration Server, and the utility operation results.

  By default, information is saved in the standard output stream (stdout). If the key is not in use, settings, results, and error messages are displayed on the screen.
- `-sp`—Shows the password for the user's authentication on the proxy server.

  The key is in use if connection to the Administration Server is established through a proxy server.
- `-savecert <file name>`—Saves the certificate used to access the Administration Server, in a specified file.
- `-restart`—Starts Network Agent after the utility has completed.
- `-sendhb`—Starts the synchronization of Network Agent with Administration Server.

After startup, the klnagchk utility accesses the configuration files of Network Agent and displays the connection parameters. These parameters are specified during the Network Agent installation and in the Network Agent policy settings:

- `Current device`—Windows network name of the client device.
- `Network Agent version`—Full number of the Network Agent version (with patches) installed on the device.
- `Server address`—Address of Administration Server.
- `Use SSL`—Parameter that indicates whether a secure connection is used when connecting to the Administration Server.

  Possible values:

  - 0—Secure connection is not used.
  - 1—Secure connection is used.
- `Compress traffic`—Parameter that indicates whether the traffic between the client device and Administration Server is compressed.
- `Server SSL ports`—Numbers of valid ports for communication with Administration Server when using a secure connection.
- `Server ports`—Numbers of valid ports for communication with the Administration Server when using an ordinary connection.
- `Use proxy server`—Parameter that indicates whether a proxy server is used.

  Possible values:

  - 0—Proxy server is not used.
  - 1—Proxy server is used.
- `Address`—Address and port of the proxy server, separated by a colon. This parameter is displayed only if a proxy server is used.
- `User name`—User name for accessing the proxy server. This parameter is displayed only if a proxy server is used.
- `Password`—Password for accessing the proxy server. This parameter is displayed only if a proxy server is used. To show the proxy server password, you need to use the `sp` key in the command.
- `Certificate`—Parameter that indicates whether the client device has an Administration Server certificate. A certificate may not exist, for example, if Network Agent has never successfully connected to Administration Server.

  Possible values:

  - `not installed`—Client device does not have an Administration Server certificate.
  - `present`—Client device has an Administration Server certificate.
- `Open UDP port`—Parameter that indicates whether Network Agent uses the UDP port to receive synchronization requests from Administration Server.

Possible values:

- 0—UDP port is closed for receiving synchronization requests from Administration Server.
- 1—UDP port is opened for receiving synchronization requests from Administration Server.

- `UDP ports`—Numbers of UDP ports that can be used by Network Agent.
- `Location name`—Network location of the device.
- `State of network location`—Parameter that indicates whether the client device can be switched from one Administration Server connection profile to another.

  Possible values:

  - `Enabled`—Administration Server connection profile can be switched for the client device.
  - `Disabled`—Administration Server connection profile cannot be switched for the client device.
- `Profile to use`—Connection profile for Administration Server.
- `Condition`—IP address and subnet mask of the network to which the client device is connected.
- `Ping period, minutes`—Standard interval between synchronizations.
- `Conn timeout, s`—Connection timeout.
- `RW timeout, s`—Connection timeout of read-write operations.
- `Host ID`—The ID of the device on the network. The `Device ID` is unique among client devices managed by the same Administration Server.
- `Locations of connection gateways`—Parameters for connecting the client device to Administration Server through the connection gateway.
- `Location of distribution points`—Parameters for connecting the client device to Administration Server through the distribution point.
- `Connection with server`—Parameter that indicates whether the connection gateway has a continuous connection to Administration Server. The parameter shows only if the client device acts as a connection gateway.

  Possible values:

  - `active`—The connection gateway has a continuous connection to Administration Server.
  - `inactive`—The connection gateway does not have a continuous connection to Administration Server.
- `Connection with server through connection gateway`—Parameter that indicates whether the connection to Administration Server through a connection gateway is established correctly. The parameter shows only if the client device acts as a connection gateway.

Possible values:

- `active`—The connection to Administration Server through a connection gateway is established correctly.
- `inactive`—The connection to Administration Server through a connection gateway is established incorrectly.

Also, the klnagchk utility output can contain one of the following lines:

- `Administration Server is installed on this device`—The klnagchk utility is run on the Administration Server device.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server`—The klnagchk utility is run on the device on which Network Agent is installed, in the connection gateway mode. The configured connection gateway is waiting for a connection from Administration Server, but Administration Server does not list the device among managed devices. You need to ensure Administration Server initiates a connection to the connection gateway.
- `This device is a connection gateway`—The klnagchk utility is run on the device that acts as a connection gateway.
- `Acts as a distribution point`—The klnagchk utility is run on the device that acts as a distribution point.

The klnagchk utility checks the status of the Network Agent service. If the service is not running, the utility stops. If the service is running, the utility displays the following connection statistics:

- `Ping count`—Number of attempts to connect the client device to Administration Server.
- `Succ. pings`—Number of successful attempts to connect the client device to Administration Server.
- `Sync count`—Number of attempts to synchronize the client device settings with the Administration Server settings.
- `Succ. syncs`—Number of successful attempts to synchronize the client device settings with Administration Server.
- `Last ping`—Date and time of the last connection.

You need to use the `Ping count` and `Succ. pings` parameters when analyzing the connection between Administration Server and Network Agent. The client device settings synchronize with the Administration Server settings only if the Administration Server settings were changed (for example, if new tasks were added or policy settings were modified). Otherwise, the `Ping count` and `Succ. pings` parameter values remain unchanged.

For more information on how to troubleshoot issues with connecting Network Agent to Administration Server, refer to Kaspersky Security Center Linux FAQ.

# Device moving rules

We recommend that you automate the allocation of devices to administration groups through *device moving rules*. A device moving rule consists of three main parts: a name, an execution condition (logical expression with the device attributes), and a target administration group. A rule moves a device to the target administration group if the device attributes meet the rule execution condition.

All device moving rules have priorities. The Administration Server checks the device attributes as to whether they meet the execution condition of each rule, in ascending order of priority. If the device attributes meet the execution condition of a rule, the device is moved to the target group, so the rule processing is complete for this device. If the device attributes meet the conditions of multiple rules, the device is moved to the target group of the rule with the highest priority (that is, has the highest rank in the list of rules).

Device moving rules can be created implicitly. For example, in the properties of an installation package or a remote installation task, you can specify the administration group to which the device must be moved after Network Agent is installed on it. Also, device moving rules can be created explicitly by the administrator of Kaspersky Security Center Linux, in the **Asset management** → **Moving rules** section.

By default, a device moving rule is intended for one-time initial allocation of devices to administration groups. The rule moves devices from the unassigned devices group only once. If a device once was moved by this rule, the rule will never move it again, even if you return the device to the unassigned devices group manually. This is the recommended way of applying moving rules.

You can move devices that have already been allocated to some of the administration groups. To do this, in the properties of a rule, clear the **Move only devices that do not belong to an administration group** check box.

Applying moving rules to devices that have already been allocated to some of the administration groups, significantly increases the load on the Administration Server.

The **Move only devices that do not belong to an administration group** check box is locked in the properties of automatically created moving rules. Such rules are created when you add the *Install application remotely* task or create a stand-alone installation package.

You can create a moving rule that would affect a single device repeatedly.

We strongly recommend that you avoid moving a single device from one group to another repeatedly (for example, in order to apply a special policy to that device, run a special group task, or update the device through a specific distribution point).

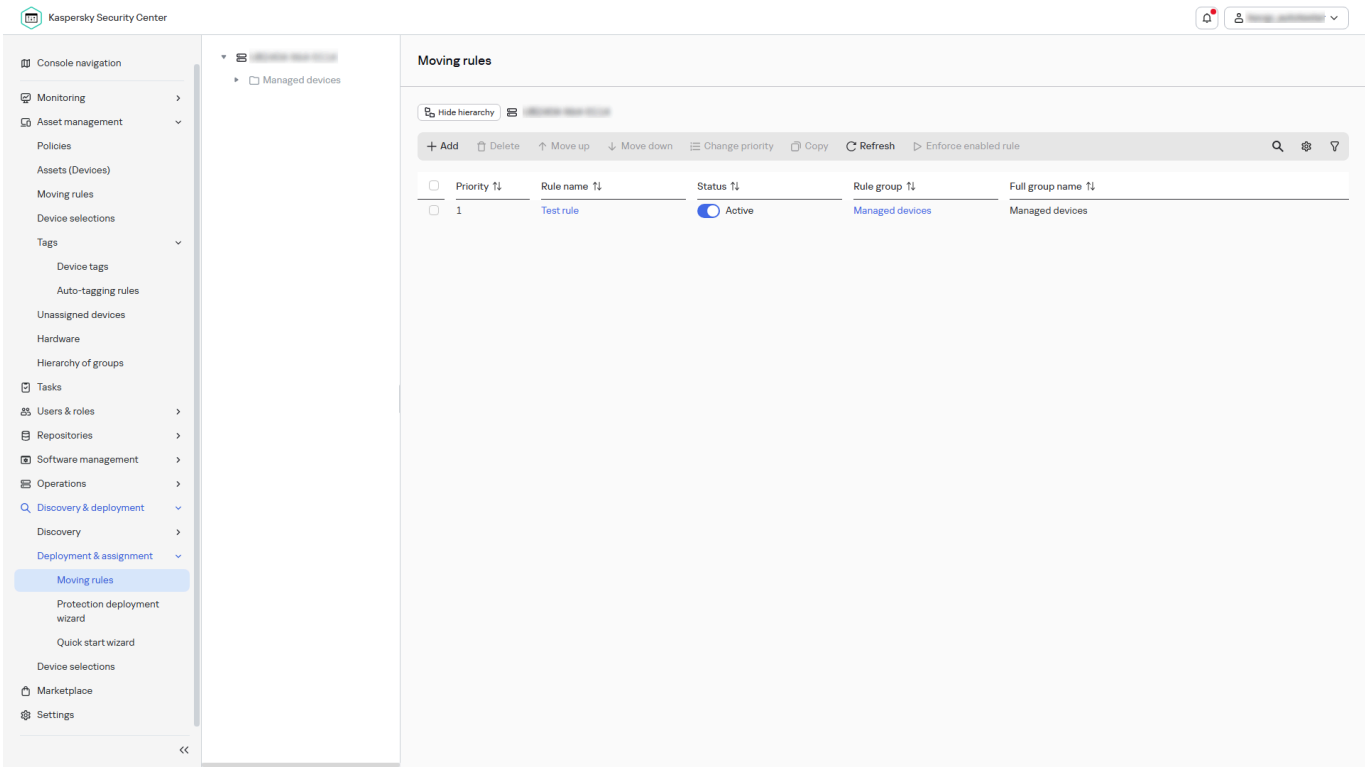
Such scenarios are not supported, because they increase the load on Administration Server and network traffic to an extreme degree. These scenarios also conflict with the operating principles of Kaspersky Security Center Linux (particularly in the area of access rights, events, and reports). Another solution must be found, for example, through the use of policy profiles, tasks for device selections, assignment of Network Agents according to the standard scenario.

# Creating device moving rules

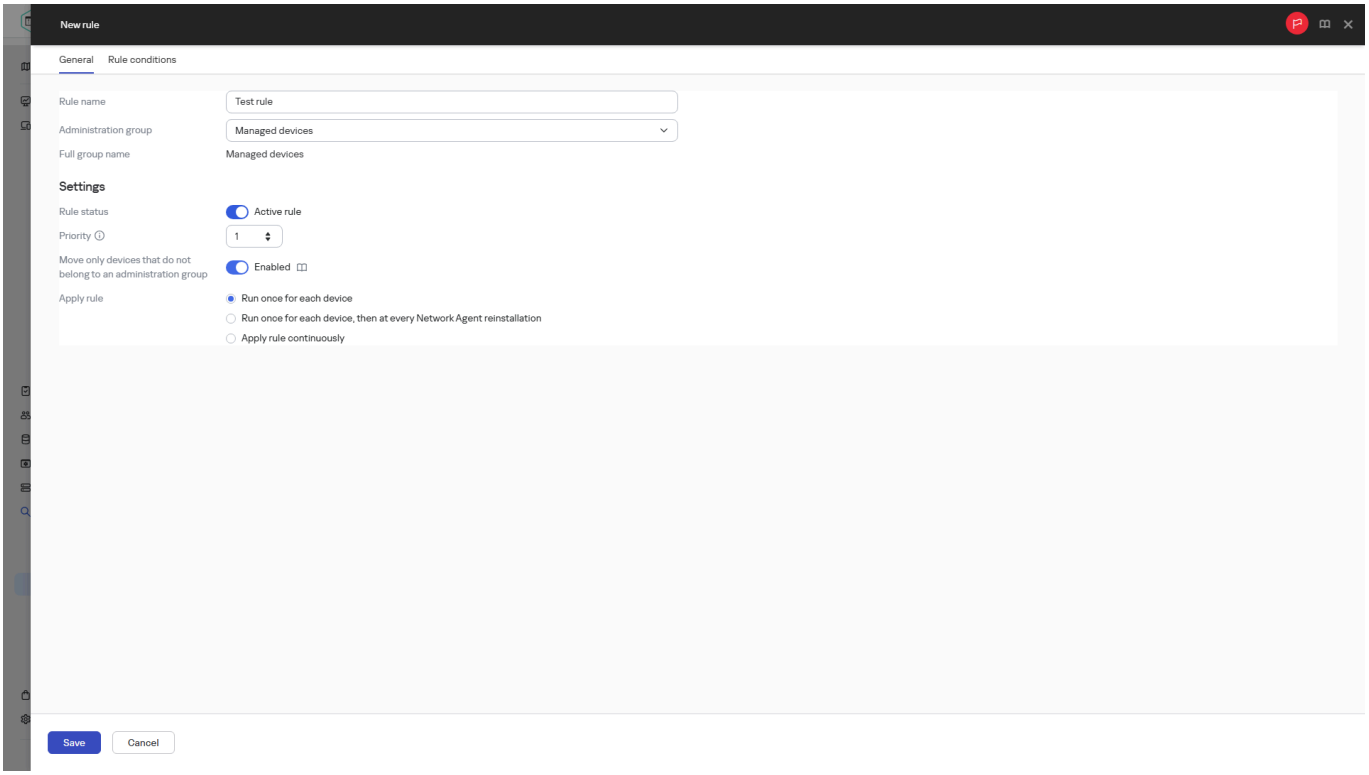
You can set up device moving rules, that is, rules that automatically allocate devices to administration groups.

*To create a moving rule:*

1. In the main menu, go to **Asset management** → **Moving rules**.




2. Click the **Add** button. The **New rule** window opens.




3. In the window that opens, specify the following information on the **General** tab:

   **Rule name**

   Enter a name for the new rule.

   If you are copying a rule, the new rule gets the same name as the source rule, but an index in () format is added to the name, for example: (1).

   **Administration group**

Select the administration group into which the devices are to be moved automatically.

**Rule status**

If this option is enabled, the rule is enabled and starts working after it is saved.

If this option is disabled, the rule is created, but not enabled. It will not work until you enable this option.

**Priority**

You can specify the moving rule's priority. The highest priority is 1. The greater the **Priority** value, the lower the rule's priority and its position in the list.

If no priority is assigned, the rule is assigned the lowest priority.

When copying a rule, the rule's copy is assigned the priority of the original rule. The original rule's priority is then increased by 1.

**Move only devices that do not belong to an administration group**

If this option is enabled, only unassigned devices will be moved to the selected group.

If this option is disabled, devices that already belong to other administration groups, as well as unassigned devices, will be moved to the selected group.

**Apply rule**

You can select one of the following options:

- **Run once for each device**

  The rule is applied once for each device that matches your criteria.

- **Run once for each device, then at every Network Agent reinstallation**

  The rule is applied once for each device that matches your criteria, then only when Network Agent is reinstalled on these devices.

- **Apply rule continuously**

  The rule is applied according to the schedule which the Administration Server sets up automatically (usually every several hours).

4. On the **Rule conditions** tab, specify at least one criterion by which the devices are moved to an administration group.

5. Click **Save**.

The moving rule is created. It is displayed in the list of moving rules.

The higher the position is on the list, the higher the priority of the rule.

*To change the priority:*

1. Select the check box of a moving rule.
2. Do one of the following:
   - Click the **Change priority** button, and specify the new priority.
   - Move the rule up or down in the list by clicking the **Move up** or **Move down** buttons.
3. Click the **Save** button.

> If the **Apply rule continuously** option is selected, the moving rule is applied regardless of the priority settings. Such rules are applied according to the schedule that the Administration Server sets up automatically.

If the device attributes meet the conditions of multiple rules, the device is moved to the target group of the rule with the highest priority (that is, has the highest rank in the list of rules).

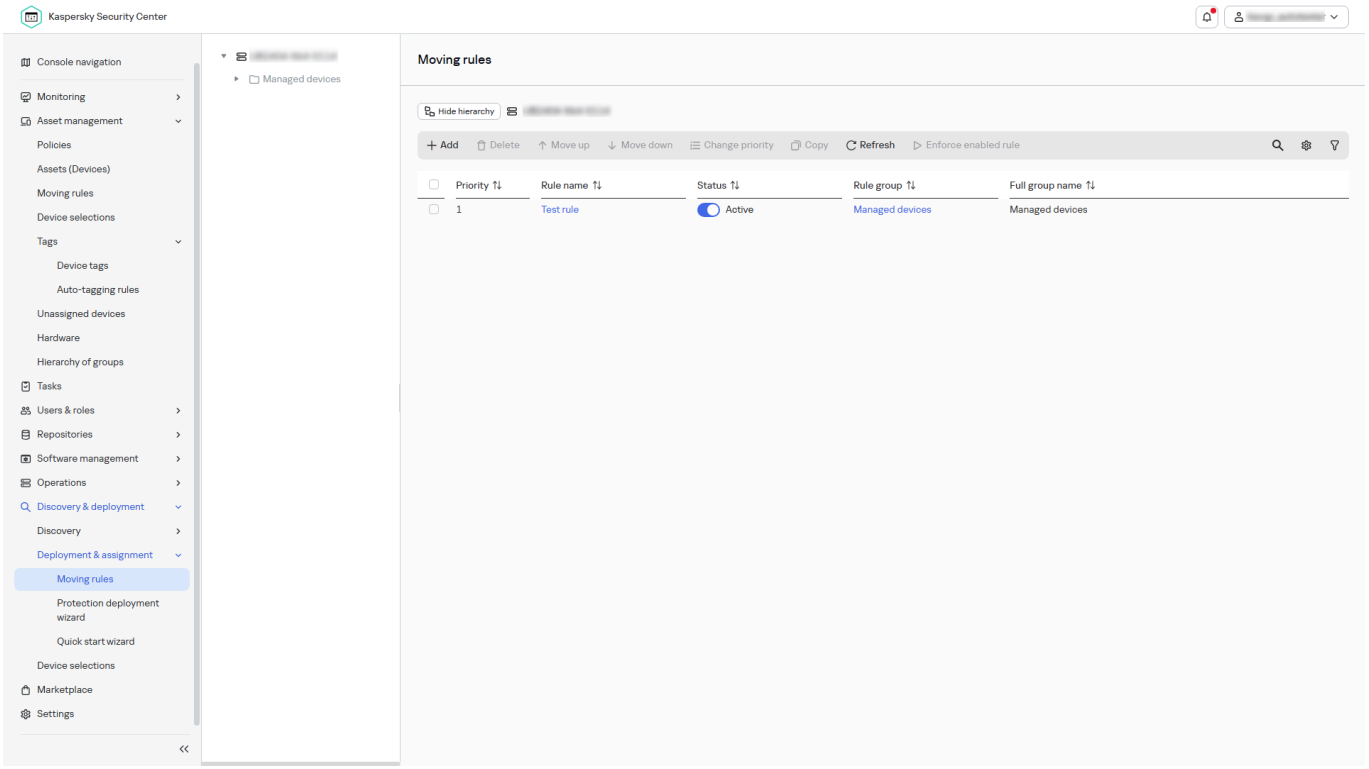
# Copying device moving rules

You can copy moving rules, for example, if you want to have several identical rules for different target administration groups.

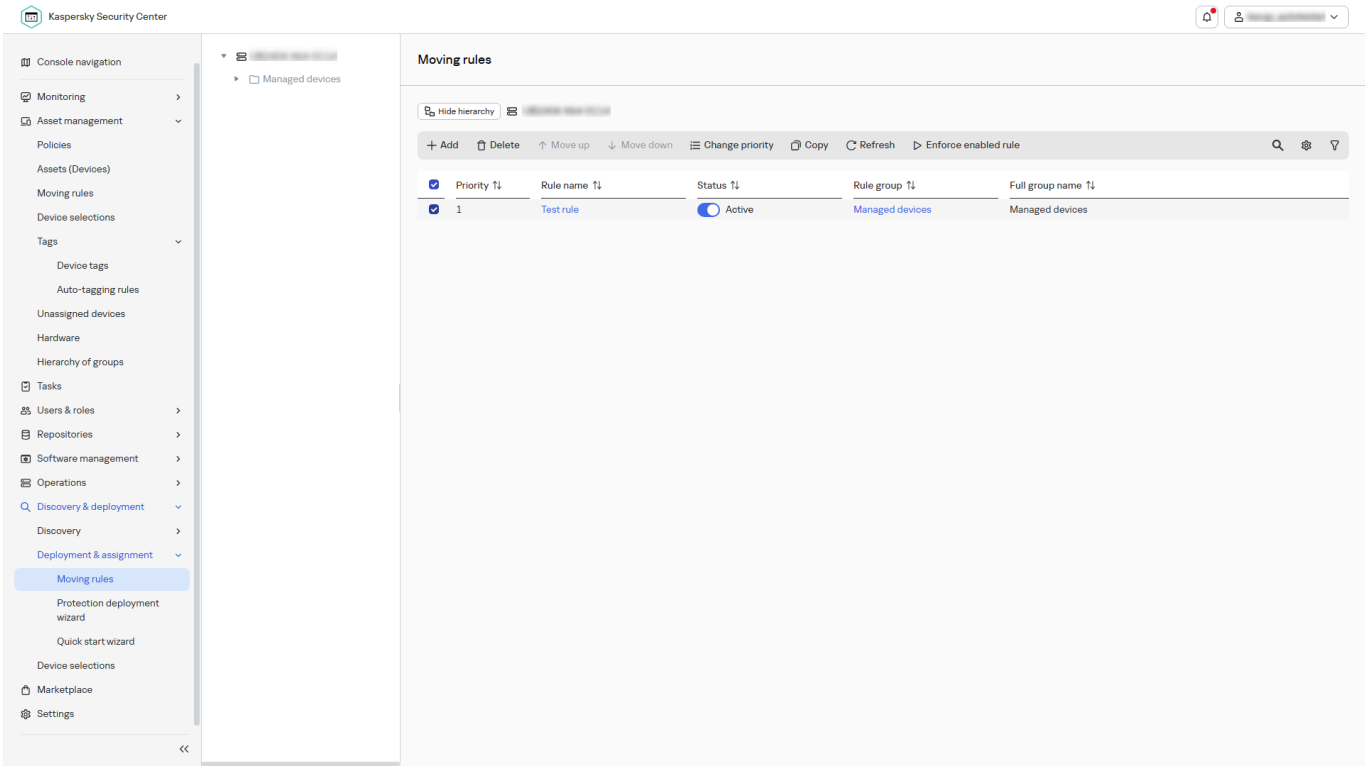
To copy an existing a moving rule:

1. Do one of the following:
   - In the main menu, go to **Asset management** → **Moving rules**.
   - In the main menu, go to **Discovery & deployment** → **Deployment & assignment** → **Moving rules**.

   The list of moving rules is displayed.




2. Select the check box next to the rule you want to copy.




3. Click the **Copy** button.

4. In the window that opens, change the following information on the **General** tab—or make no changes if you only want to copy the rule without changing its settings:

   **Rule name**

   Enter a name for the new rule.

   If you are copying a rule, the new rule gets the same name as the source rule, but an index in () format is added to the name, for example: (1).

   **Administration group**

Select the administration group into which the devices are to be moved automatically.

**Rule status**

If this option is enabled, the rule is enabled and starts working after it is saved.

If this option is disabled, the rule is created, but not enabled. It will not work until you enable this option.

**Priority**

You can specify the moving rule's priority. The highest priority is 1. The greater the **Priority** value, the lower the rule's priority and its position in the list.

If no priority is assigned, the rule is assigned the lowest priority.

When copying a rule, the rule's copy is assigned the priority of the original rule. The original rule's priority is then increased by 1.

**Move only devices that do not belong to an administration group**

If this option is enabled, only unassigned devices will be moved to the selected group.

If this option is disabled, devices that already belong to other administration groups, as well as unassigned devices, will be moved to the selected group.

**Apply rule**

You can select one of the following options:

- **Run once for each device**

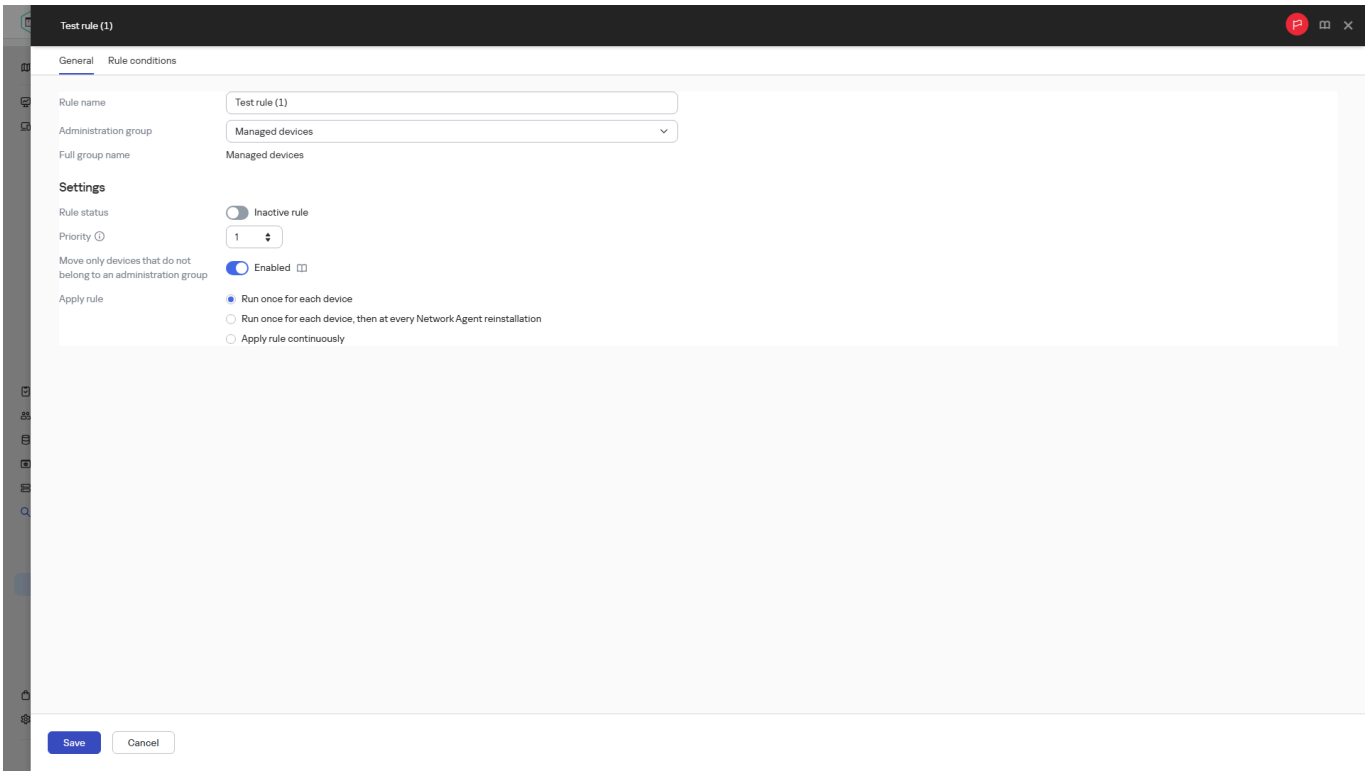
  The rule is applied once for each device that matches your criteria.

- **Run once for each device, then at every Network Agent reinstallation**

  The rule is applied once for each device that matches your criteria, then only when Network Agent is reinstalled on these devices.

- **Apply rule continuously**

  The rule is applied according to the schedule which the Administration Server sets up automatically (usually every several hours).




5. On the **Rule conditions** tab, specify at least one criterion for the devices that you want to be moved automatically.

6. Click **Save**.

The new moving rule is created. It is displayed in the list of moving rules.

# Conditions for a device moving rule

When you create or copy a rule to move client devices to administration groups, on the **Rule conditions** tab you set conditions for moving the devices. To determine which devices to move, you can use the following criteria:

- Tags assigned to client devices.
- Network parameters. For example, you can move devices with IP addresses from a specified range.
- Device owner, his or her role and security group membership.
- Managed applications installed on client devices, for instance, Network Agent or Administration Server.
- Virtual machines, which are the client devices.
- Domain controller organizational units.
- Cloud segments.

Below, you can find the description on how to specify this information in a device moving rule.

If you specify several conditions in the rule, the AND logical operator works and all the conditions apply at the same time. If you do not select any options or keep some fields blank, such conditions do not apply.

### Tags tab

On this tab, you can configure a device moving rule based on device tags that were previously added to the descriptions of client devices. To do this, select the required tags. Also, you can enable the following options:

**Apply to devices without the specified tags**

If this option is enabled, all devices with the specified tags are excluded from a device moving rule. If this option is disabled, the device moving rule applies to devices with all the selected tags.

By default, this option is disabled.

**Apply if at least one specified tag matches**

If this option is enabled, a device moving rule applies to client devices with at least one of the selected tags. If this option is disabled, the device moving rule applies to devices with all the selected tags.

By default, this option is disabled.

### Network tab

On this tab, you can specify the network data of devices that a device moving rule considers:

**Device name on the Windows network**

Windows network name (NetBIOS name) of the device, or the IPv4 or IPv6 address.

**Windows domain**

A device moving rule applies to all devices included in the specified Windows domain.

**DNS name of the device**

DNS domain name of the client device that you want to move. Fill this field if your network includes a DNS server.

> If case sensitive collation is set for the database that you use for Kaspersky Security Center Linux, keep case when you specify a device DNS name. Otherwise, the device moving rule will not work.

**DNS domain**

A device moving rule applies to all devices included in the specified main DNS suffix. Fill this field if your network includes a DNS server.

**IP range**

If this option is enabled, you can enter the initial and final IP addresses of the IP range in which the relevant devices must be included.

By default, this option is disabled.

**IP address for connection to Administration Server**

If this option is enabled, you can set the IP addresses by which client devices are connected to Administration Server. To do this, specify the IP range that includes all necessary IP addresses.

By default, this option is disabled.

**Device is located in a subgroup of the Domains group**

If this option is enabled, you can select a subgroup of the Domains group. The relevant devices must be located in the selected subgroup.

By default, this option is disabled.

**Device is in IP range**

If this option is enabled, you can select an IP range that you previously added in the **IP ranges** section. The relevant devices must be included in the selected IP range.

By default, this option is disabled.

**Connection profile changed**

Select one of the following values:

- **Yes**. A device moving rule only applies to client devices with a changed connection profile.
- **No**. The device moving rule only applies to the client devices whose connection profile has not changed.
- **No value is selected**. The condition does not apply.

**Managed by a different Administration Server**

Select one of the following values:

- **Yes**. A device moving rule only applies to client devices managed by other Administration Servers. These Servers are different from the Server on which you configure the device moving rule.
- **No**. The device moving rule only applies to client devices managed by the current Administration Server.
- **No value is selected**. The condition does not apply.

Device owner tab

On this tab, you can configure a device moving rule based on the device owner, security group membership, and role:

**Device owner**

Select a device owner's user name from an internal security group. Learn more about users and user roles in this section.

> No more than one user can be registered as the device owner.

**Device owner's membership in Active Directory security group**

Select an external Active Directory security group that the device owner belongs to.

The user can be a part of an Active Directory security group or a part of a group that is included in this Active Directory security group.

**Device owner's role**

Select the device owner's assigned role. Learn more about user roles in this article.

**Device owner's membership in an internal security group**

Select an internal security group that the device owner belongs to.

## Applications tab

On this tab, you can configure a device moving rule based on the managed applications and operating systems installed on client devices:

**Network Agent is installed**

Select one of the following values:

- **Yes**. A device moving rule only applies to client devices with Network Agent installed.
- **No**. The device moving rule only applies to client devices on which Network Agent is not installed.
- **No value is selected**. The condition does not apply.

**Applications**

Specify what managed applications should be installed on client devices, so a device moving rule applies to these devices. For example, you can select **Kaspersky Security Center 17 Network Agent** or **Kaspersky Security Center 17 Administration Server**.

If you do not select any managed application, the condition does not apply.

**OS version**

You can cull client devices based on the operating system version. For this purpose, specify operating systems that should be installed on the client devices. As a result, a device moving rule applies to the client devices with the selected operating systems.

If you do not enable this option, the condition does not apply. By default, this option is disabled.

**OS architecture**

You can cull client devices by the operating system bit sizes. In the **Operating system architecture** field, you can select one of the following values:

- **Unknown**
- **x86**
- **AMD64**
- **IA64**

*To check the operating system architecture of the client devices:*

1. In the main menu, go to the **Asset management** → **Managed devices** section.
2. Click the **Columns settings** button ( ⚙ ) on the right.
3. Select the **OS architecture** option, and then click the **Save** button.

   After that, the operating system architecture is displayed for every managed device.

**OS package manager**

You can cull client devices by the operating system package manager. In the **OS package manager** field, you can select one of the following values:

- rpm—for devices running Red Hat Enterprise Linux, CentOS, Fedora, SUSE, Oracle Linux operating systems
- apt (dpkg)—for devices running Debian, Ubuntu, Kali operating systems
- pkg—for devices running FreeBSD, OpenBSD operating systems

*To check the operating system package manager of the client devices:*

1. In the main menu, go to the **Asset management** → **Managed devices** section.
2. Click the **Columns settings** button ( ⚙ ) on the right.
3. Select the **OS package manager** option, and then click the **Save** button.

The operating system package manager is displayed for every managed device.

**OS service pack version**

In this field, you can specify the package version of the operating system (in the *X.Y* format), which will determine how the moving rule is applied to the device. By default, no version value is specified.

**User certificate**

Select one of the following values:

- **Installed**. A device moving rule only applies to mobile devices with a mobile certificate.
- **Not installed**. The device moving rule only applies to mobile devices without a mobile certificate.
- **No value is selected**. The condition does not apply.

**OS build**

This setting is applicable to Windows operating systems only.

You can specify whether the selected operating system must have an equal, earlier, or later release number. You can also configure a device moving rule for all build numbers except the specified one.

**OS release number**

This setting is applicable to Windows operating systems only.

You can specify whether the selected operating system must have an equal, earlier, or later release number. You can also configure a device moving rule for all release numbers except the specified one.

### Virtual machines tab

On this tab, you can configure a device moving rule according to whether client devices are virtual machines or part of a virtual desktop infrastructure (VDI):

**This is a virtual machine**

In the drop-down list, you can select one of the following:

- **N/A**. The condition does not apply.
- **No**. Move devices that are not virtual machines.
- **Yes**. Move devices that are virtual machines.

**Virtual machine type**

**Part of Virtual Desktop Infrastructure**

In the drop-down list, you can select one of the following:

- **N/A**. The condition does not apply.
- **No**. Move devices that are not part of VDI.
- **Yes**. Move devices that are part of VDI.

### Domain controller tab

On this tab, you can specify that it is necessary to move devices included in the domain organizational unit. You can also move devices from all child organizational units of the specified domain organizational unit:

**Device is included in the following organizational unit**

If this option is enabled, a device moving rule applies to devices from the domain controller organizational unit specified in the list under the option.

By default, this option is disabled.

**Include child organizational units**

If this option is enabled, the selection includes devices from all child organizational units of the specified domain controller organizational unit.

By default, this option is disabled.

**Move devices from child units to corresponding subgroups**

**Create subgroups corresponding to containers of newly detected devices**

**Delete subgroups that are not present in the domain**

**Device is included in the following domain security group**

If this option is enabled, a device moving rule applies to devices from the domain security group specified in the list under the option.

By default, this option is disabled.

## Cloud segments tab

On this tab, you can specify that it is necessary to move devices included in the cloud segment. You can also move devices from all child organizational units of the specified domain organizational unit:

**Device is in a cloud segment**

If you select this option, a device moving rule applies to the client devices that belong to a cloud segment. You can select the required cloud segment up to a subnet in the list under the option.

By default, this option is disabled.

**Include child objects**

If this option is enabled, the selection includes devices from all child organizational units of the specified cloud segment.

By default, this option is disabled.

**Move devices from nested objects to corresponding subgroups**

**Create subgroups corresponding to containers of newly detected devices**

**Delete subgroups for which no match is found in the cloud segments**

**Device discovered by using the API**

In the drop-down list, you can select one of the following:

- No value is selected. The condition does not apply.
- **No**. Move devices that are not discovered by using the API.
- **AWS**. Move devices that are discovered by AWS API.
- **Azure**. Move devices that are discovered by Azure API.
- **Google Cloud**. Move devices that are discovered by Google Cloud API.

After that, depending on the selected value, you can fill in the following fields:

- **Cloud device subnet**.
- **Cloud device availability zone**.
- **Cloud device placement group**.

The Custom parameters tab

> Custom settings are available only with the Kaspersky Mobile Devices Protection and Management plug-in 10.59.4.32 or later installed.

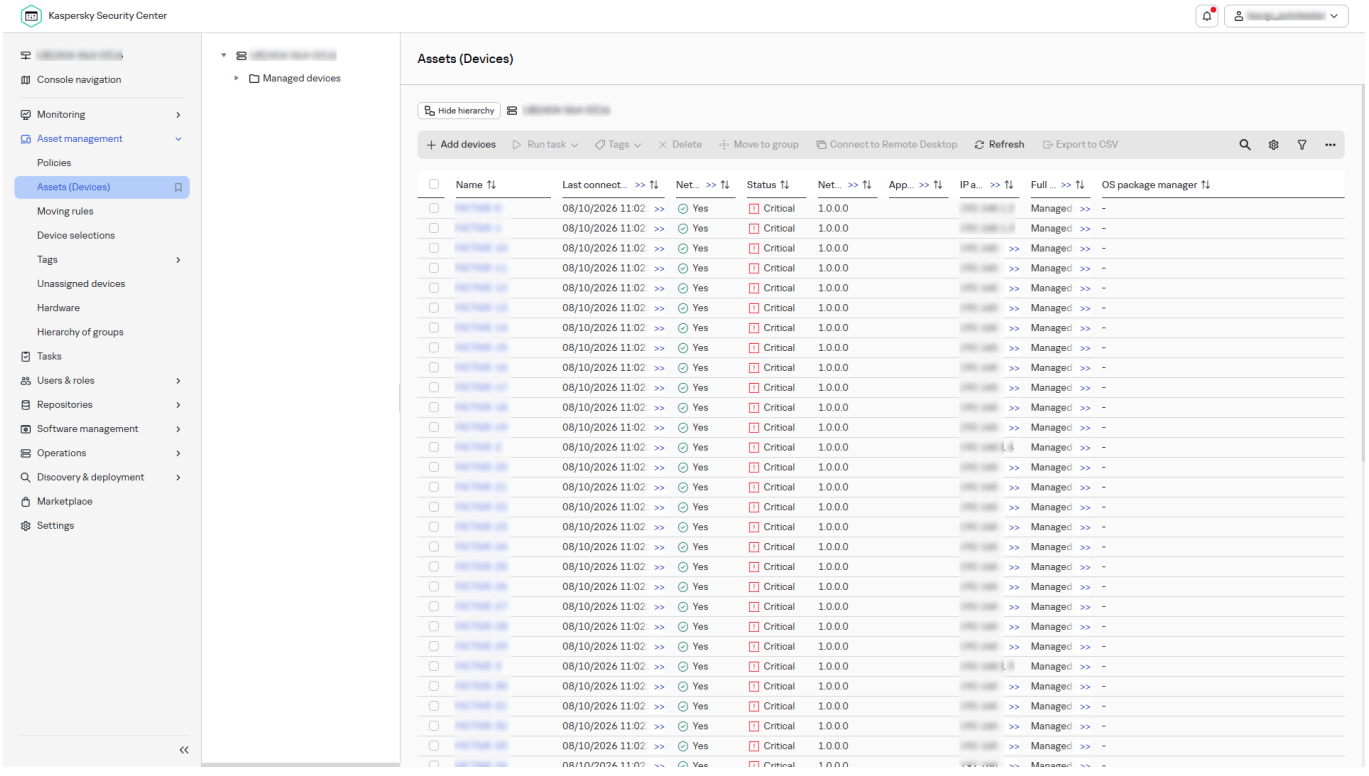
On this tab, you can configure the rule for moving Android devices based on the values of custom settings. For detailed information on using custom settings, refer to the Kaspersky Secure Mobility Management Help.

# Adding devices to an administration group manually

You can move devices to administration groups automatically by creating device moving rules or manually by moving devices from one administration group to another or by adding devices to a selected administration group. This section describes how to manually add devices to an administration group.

*To add manually one or more devices to a selected administration group:*

1. In the main menu, go to **Asset management** → **Managed devices**.




The list of managed devices

2. Select the administration group to which you want to add the devices:

   - For the root group:

     In this case you can proceed to the next step.

   - For a subgroup:

     a. Click the **Show hierarchy** button at the top of the page.

        The button name changes to **Hide hierarchy**.

     b. In the window that opens, click the name of the subgroup.

     The path to the selected group is displayed at the top of the page. If necessary, you can click a link with the administration group name to go to the group. By default, the last link in the path is inactive. Also, you can close the hierarchy window by clicking the **Hide hierarchy** button.

3. Click the **Add devices** button.

   The Move devices wizard starts.

4. Make a list of the devices that you want to add to the administration group.

   > You can add only devices for which information has already been added to the Administration Server database either upon connection of the device or after device discovery.

   Select how you want to add devices to the list:

   - Click the **Add devices** button, and then specify the devices in one of the following ways:

     - Select devices from the list of devices detected by the Administration Server.
     - Specify a device IP address or an IP range.

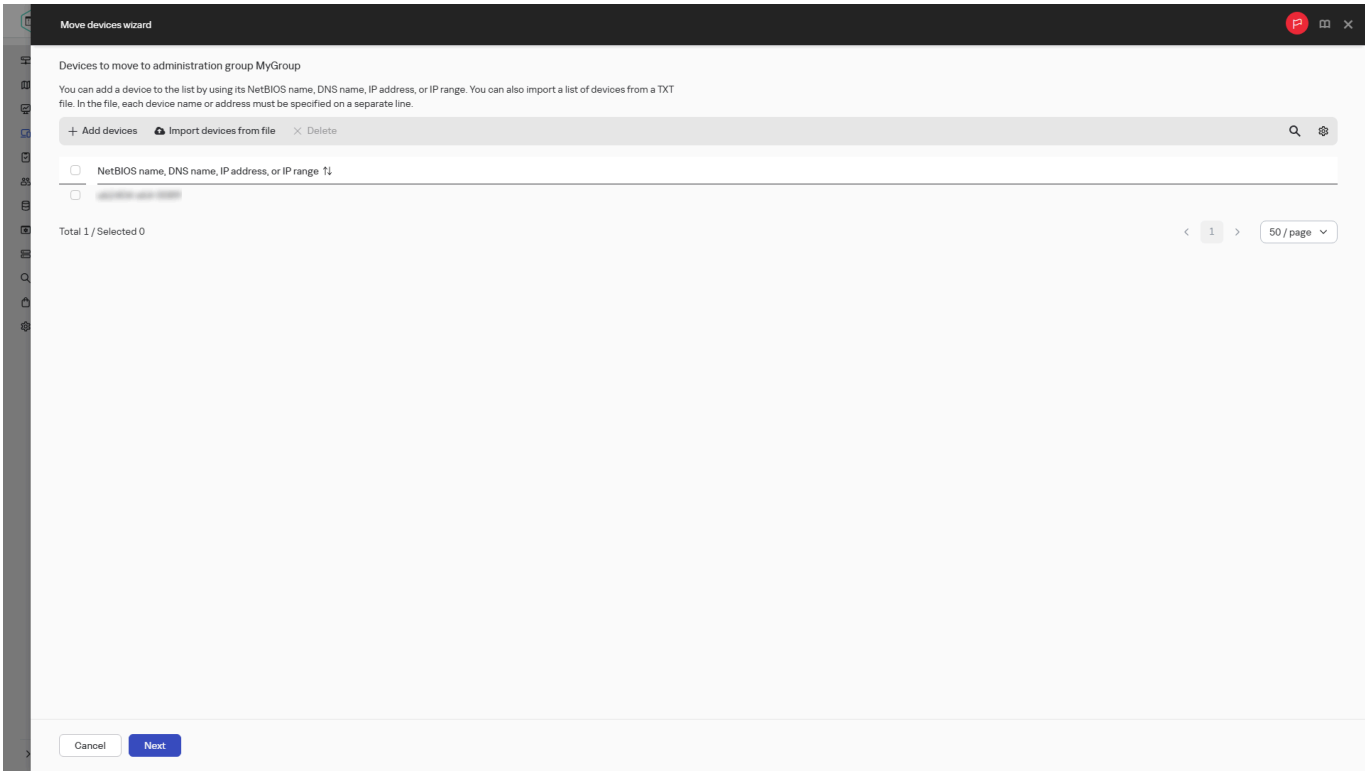
       > The IP range must not contain more than 1,048,576 addresses.

     - Specify a device DNS name.

       > The device name field must not contain space characters, backspace characters, or the following prohibited characters: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Click the **Import devices from file** button to import a list of devices from a .txt file. Each device address or name must be specified on a separate line.

  The file must not contain space characters, backspace characters, or the following prohibited characters: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %




Selecting devices to move to the administration group

5. View the list of devices to be added to the administration group. You can edit the list by adding or removing devices.

6. After making sure that the list is correct, click the **Next** button.

   The wizard processes the device list and displays the result. The successfully processed devices are added to the administration group and are displayed in the list of devices under names generated by Administration Server.

# Moving devices or clusters to an administration group manually

You can move devices from one administration group to another, or from the group of unassigned devices to an administration group.

You can also move clusters or server arrays from one administration group to another. When you move a cluster or server array to another group, all of its nodes move with it, because a cluster and any of its nodes always belong to the same administration group. When you select a single cluster node on the **Devices** tab, the **Move to group** button becomes unavailable.

*To move one or several devices or clusters to a selected administration group:*

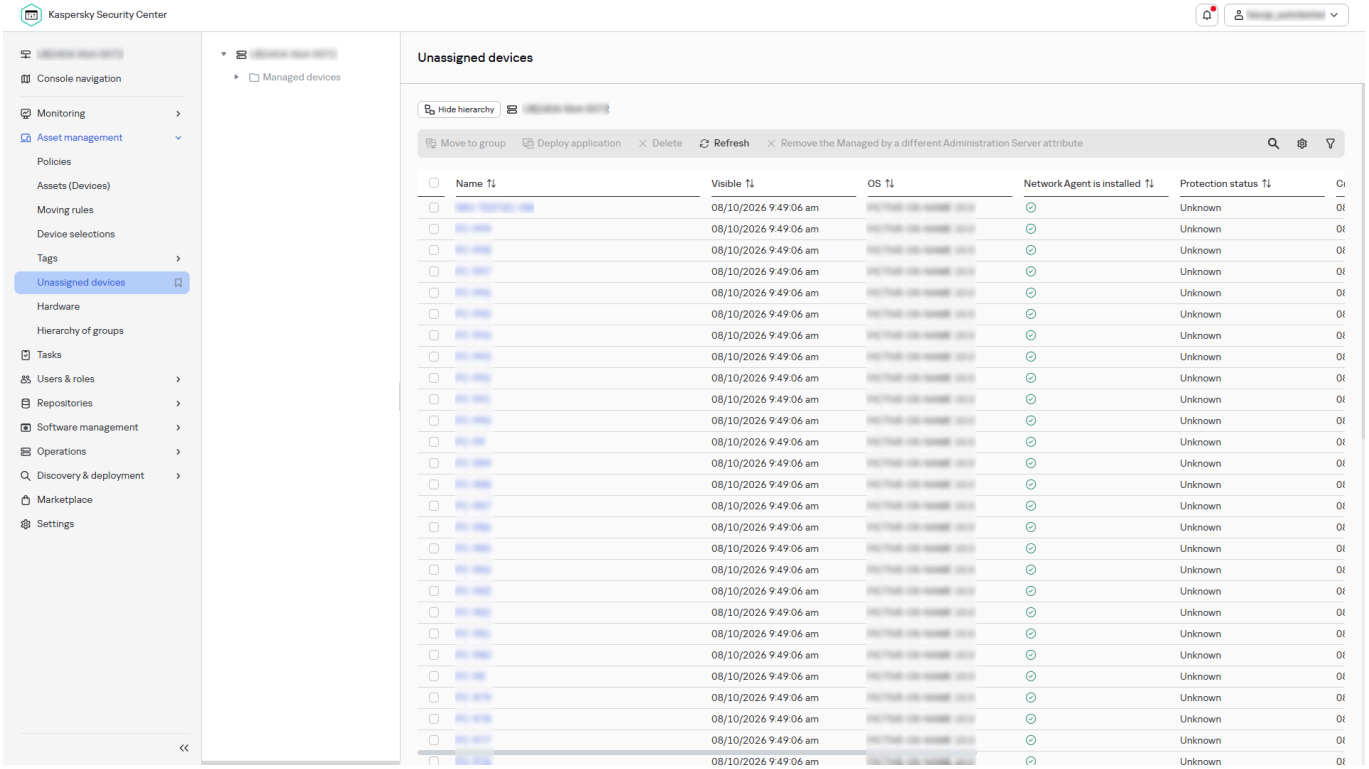
1. Open the administration group from which you want to move the devices. To do so, follow one of these steps:

   - To open an administration group, in the main menu, go to **Asset management** → **Managed devices**, and then select the required administration group.

     - For the root group, you can proceed to the next step.

     - For a subgroup, click the **Show hierarchy** button at the top of the page, and then, in the window that opens, select a required administration group.

   - To open the **Unassigned devices** group, in the main menu, go to **Asset management** → **Unassigned devices**.




The list of unassigned devices

2. If the administration group contains clusters or server arrays, the **Managed devices** section is divided into two tabs—the **Devices** tab and the **Clusters and server arrays** tab. Open the tab for the object that you want to move.

3. Select the check boxes next to the devices or clusters that you want to move to a different group.

4. Click the **Move to group** button.

5. In the hierarchy of administration groups, select the check box next to the administration group to which you want to move the selected devices or clusters.

6. Click the **Move** button.

The selected devices or clusters are moved to the selected administration group.

# About clusters and server arrays

Kaspersky Security Center Linux supports cluster technology. If Network Agent sends information to Administration Server confirming that an application installed on a client device is part of a server array, this client device becomes a cluster node.

If an administration group contains clusters or server arrays, the **Managed devices** page displays two tabs—one for individual devices, and one for clusters and server arrays. After the managed devices are detected as cluster nodes, the cluster is added as an individual object to the **Clusters and server arrays** tab.

The cluster or server array nodes are listed on the **Devices** tab, along with other managed devices. You can view properties of the nodes as individual devices and perform other operations, but you cannot delete a cluster node or move it to another administration group separately from its cluster. You can only delete or move an entire cluster.

You can perform the following operations with clusters or server arrays:

- View properties
- Move the cluster or server array to another administration group

  When you move a cluster or server array to another group, all of its nodes move with it, because a cluster and any of its nodes always belong to the same administration group.
- Delete

  It is reasonable to delete a cluster or server array only when the cluster or server array does not exist in the organization network any longer. If a cluster is still visible on your network and Network Agent and the Kaspersky security application are still installed on the cluster nodes, Kaspersky Security Center Linux returns the deleted cluster and its nodes back to the list of managed devices automatically.

# Properties of a cluster or server array

*To view the settings of a cluster or server array:*

1. In the main menu, go to **Asset management** → **Managed devices** → **Clusters and server arrays**.

   The list of clusters and server arrays is displayed.
2. Click the name of the required cluster or server array.

The properties window of the selected cluster or server array is displayed.

### General

The **General** section displays general information about the cluster or server array. Information is provided on the basis of data received during the last synchronization of the cluster nodes with the Administration Server:

#### Name

**Description**

**Windows domain**

Windows domain or workgroup, which contains the cluster or server array.

**NetBIOS name**

Windows network name of the cluster or server array.

**DNS name**

Name of the DNS domain of the cluster or server array.

### Tasks

In the **Tasks** tab, you can manage the tasks assigned to the cluster or server array: view the list of existing tasks; create new ones; remove, start, and stop tasks; modify task settings; and view execution results. The listed tasks relate to the Kaspersky security application installed on the cluster nodes. Kaspersky Security Center Linux receives the task list and the task status details from the cluster nodes. If a connection is not established, the status is not displayed.

### Nodes

This tab displays a list of nodes included into the cluster or server array. You can click a node name to view the device properties window.

**Kaspersky application**

The properties window may also contain additional tabs with the information and settings related to the Kaspersky security application installed on the cluster nodes.

# Adjustment of distribution points and connection gateways

A structure of administration groups in Kaspersky Security Center Linux performs the following functions:

- Sets the scope of policies

  There is an alternate way of applying relevant settings on devices, by using *policy profiles*.

- Sets the scope of group tasks

  There is an approach to defining the scope of group tasks that is not based on a hierarchy of administration groups: use of tasks for device selections and tasks for specific devices.

- Sets access rights to devices, virtual Administration Servers, and secondary Administration Servers
- Assigns distribution points

When building the structure of administration groups, you must take into account the topology of the organization's network for the optimum assignment of distribution points. The optimum distribution of distribution points allows you to save traffic on the organization's network.

Depending on the organizational schema and network topology, the following standard configurations can be applied to the structure of administration groups:

- Single office
- Multiple small remote offices

Devices functioning as distribution points must be protected, including physical protection, against any unauthorized access.

# About distribution points

A device with Network Agent installed can be used as a distribution point. In this mode, Network Agent can distribute updates, which can be retrieved either from the Administration Server or from Kaspersky servers. In the latter case, configure update download for a distribution point.

Deployment of distribution points on an organization's network has the following objectives:

- Reducing the load on the Administration Server.
- Optimizing traffic.
- Providing the Administration Server with access to devices in hard-to-reach spots of the organization's network. The availability of a distribution point on the network behind a NAT (in relation to the Administration Server) allows the Administration Server to perform the following actions:
  - Send notifications to devices over UDP on the IPv4 or IPv6 network
  - Poll the IPv4 or IPv6 network
  - Perform initial deployment
  - Act as a push server

A distribution point is assigned for an administration group. In this case, the scope of the distribution point includes all devices within the administration group and all of its subgroups. However, the device acting as the distribution point may not be included in the administration group to which it has been assigned.

You can make a distribution point function as a connection gateway. In this case, devices in the scope of the distribution point will be connected to the Administration Server through the gateway, not directly. This mode can be useful in scenarios that do not allow the establishment of a direct connection between the Administration Server and managed devices.

If you use a Linux-based device as a distribution point, we strongly recommend to increase the limit of file descriptors for the klnagent service, because if the scope of the distribution point includes many devices, the default maximum number of files that can be opened may not be enough.

# Standard configuration of distribution points: Single office

In a standard "single-office" configuration, all devices are on the organization's network so they can "see" each other. The organization's network may consist of a few separate parts (networks or network segments) linked by narrow channels.

The following methods of building the structure of administration groups are possible:

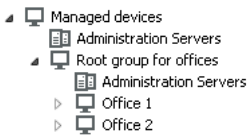
- Building the structure of administration groups taking into account the network topology. The structure of administration groups may not reflect the network topology with absolute precision. A match between the separate parts of the network and certain administration groups would be enough. You can use automatic assignment of distribution points or assign them manually.

- Building the structure of administration groups, without taking the network topology into account. In this case, you must disable automatic assignment of distribution points, and then assign one or several devices to act as distribution points for a root administration group in each of the separate parts of the network, for example, for the **Managed devices** group. All distribution points will be at the same level and will feature the same scope spanning all devices on the organization's network. In this case, each Network Agent will connect to the distribution point that has the shortest route. The route to a distribution point can be traced with the tracert utility.

# Standard configuration of distribution points: Multiple small remote offices

This standard configuration provides for a number of small remote offices, which may communicate with the head office over the internet. Each remote office is located behind the NAT, that is, connection from one remote office to another is not possible because offices are isolated from one another.

The configuration must be reflected in the structure of administration groups: a separate administration group must be created for each remote office (groups **Office 1** and **Office 2** in the figure below).




Remote offices are included in the administration group structure

One or multiple distribution points must be assigned to each administration group that correspond to an office. Distribution points must be devices at the remote office that have a sufficient amount of free disk space. Devices deployed in the **Office 1** group, for example, will access distribution points assigned to the **Office 1** administration group.

If some users move between offices physically, with their laptops, you must select two or more devices (in addition to the existing distribution points) in each remote office and assign them to act as distribution points for a top-level administration group (**Root group for offices** in the figure above).

Example: A laptop is deployed in the **Office 1** administration group and then is moved physically to the office that corresponds to the **Office 2** administration group. After the laptop is moved, Network Agent attempts to access the distribution points assigned to the **Office 1** group, but those distribution points are unavailable. Then, Network Agent starts attempting to access the distribution points that have been assigned to the **Root group for offices**. Because remote offices are isolated from one another, attempts to access distribution points assigned to the **Root group for offices** administration group will only be successful when Network Agent attempts to access distribution points in the **Office 2** group. That is, the laptop will remain in the administration group that corresponds to the initial office, but the laptop will use the distribution point of the office where it is physically located at the moment.

# Calculating the number and configuration of distribution points

The more client devices a network contains, the more distribution points it requires. We recommend that you not disable automatic assignment of distribution points. When automatic assignment of distribution points is enabled, Administration Server assigns distribution points if the number of client devices is quite large and defines their configuration.

## Using exclusively assigned distribution points

If you plan to use certain specific devices as distribution points (that is, exclusively assigned servers), you can opt out of using automatic assignment of distribution points. In this case, make sure that the devices that you intend to make distribution points have sufficient volume of free disk space, are not shut down regularly, and have Sleep mode disabled.

Number of dedicated distribution points in a network containing one network segment, depending on the number of devices in the network

| Number of client devices per network segment | Number of distribution points |
|---|---|
| Less than 300 | 0 (Do not assign distribution points) |
| More than 300 | Acceptable: (N/10,000 + 1), recommended: (N/5000 + 2), where N is the number of networked devices |

Number of dedicated distribution points in a network containing multiple network segments, depending on the number of devices in the network

| Number of client devices in each network segment | Number of distribution points |
|---|---|
| Less than 10 | 0 (Do not assign distribution points) |
| 10–100 | 1 |
| More than 100 | Acceptable: (N/10,000 + 1), recommended: (N/5000 + 2), where N is the number of networked devices |

### Using standard client devices (workstations) as distribution points

If you plan to use standard client devices (that is, workstations) as distribution points, we recommend that you assign distribution points as shown in the tables below in order to avoid excessive load on the communication channels and on Administration Server:

Number of workstations functioning as distribution points on a network that contains a single network segment, based on the number of networked devices

| Number of client devices per network segment | Number of distribution points |
|---|---|
| Less than 300 | 0 (Do not assign distribution points) |
| More than 300 | (N/300 + 1), where N is the number of networked devices; there must be at least 3 distribution points |

Number of workstations functioning as distribution points on a network that contains multiple network segments, based on the number of networked devices

| Number of client devices per network segment | Number of distribution points |
|---|---|
| Less than 10 | 0 (Do not assign distribution points) |
| 10–30 | 1 |
| 31–300 | 2 |
| More than 300 | (N/300 + 1), where N is the number of networked devices; there must be at least 3 distribution points |

If a distribution point is shut down (or not available for some other reason), the managed devices in its scope can access the Administration Server for updates.

## Assigning distribution points automatically

We recommend that you assign distribution points automatically. In this case, Kaspersky Security Center Linux will select on its own which devices must be assigned distribution points.

Devices running Microsoft Windows on Arm cannot act as distribution points.

*To assign distribution points automatically:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Distribution points** section.

3. Select the **Automatically assign distribution points** option.

   If automatic assignment of devices as distribution points is enabled, you cannot configure distribution points manually or edit the list of distribution points.

4. Click the **Save** button.

   Administration Server assigns and configures distribution points automatically.

# Assigning distribution points manually

Kaspersky Security Center Linux allows you to manually assign devices to act as distribution points.

We recommend that you assign distribution points automatically. In this case, Kaspersky Security Center Linux will select on its own which devices must be assigned distribution points. However, if you have to opt out of assigning distribution points automatically for any reason (for example, if you want to use exclusively assigned servers), you can assign distribution points manually after you Calculating the number and configuration of distribution points.

Devices functioning as distribution points must be protected, including physical protection, against any unauthorized access.

Devices running Microsoft Windows on Arm cannot act as distribution points.

*To manually assign a device to act as distribution point:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Distribution points** section.

3. Select the **Manually assign distribution points** option.

4. Click the **Assign** button.

5. Select the device that you want to make a distribution point.

   When selecting a device, keep in mind the operation features of distribution points and the requirements set for the device that acts as distribution point.

6. Select the administration group that you want to include in the scope of the selected distribution point.

7. Click **OK**.

   The distribution point that you have added will be displayed in the list of distribution points, in the **Distribution points** section.

8. Click the newly added distribution point in the list to open its properties window.

9. Configure the distribution point in the properties window:

- The **General** section contains the settings of interaction between the distribution point and client devices.

  **SSL port**

  The number of the SSL port for encrypted connection between client devices and the distribution point using SSL.

  The default port number is 13000.

  **Enabled**

  If this option is enabled, IP multicasting will be used for automatic distribution of installation packages to client devices within the group.

  IP multicasting decreases the time required to install an application from an installation package to a group of client devices, but increases the installation time when you install an application to a single client device.

  **IP multicast address**

  IP address that will be used for multicasting. You can define an IP address in the range of 224.0.0.0 – 239.255.255.255

  By default, Kaspersky Security Center Linux automatically assigns a unique IP multicast address within the given range.

  **IP multicast port number**

  Number of the port for IP multicasting.

  By default, the port number is 15001. If the device with Administration Server installed is specified as the distribution point, port 13001 is used for SSL connection by default.

  **Distribution point address for remote devices**

  The network address through which remote devices connect to the distribution point.

  **Enabled**

  Updates are distributed to managed devices from the following sources:

  - This distribution point, if this option is enabled.
  - Other distribution points, Administration Server, or Kaspersky update servers, if this option is disabled.

  If you use distribution points to deploy updates, you can save traffic because you reduce the number of downloads. Also, you can relieve the load on the Administration Server and relocate the load between the distribution points. You can Calculating the number and configuration of distribution points the number of distribution points for your network to optimize the traffic and load.

  If you disable this option, the number of update downloads and load on the Administration Server may increase. By default, the option is enabled.

  **Enabled**

  Installation packages are distributed to managed devices from the following sources:

  - This distribution point, if this option is enabled.
  - Other distribution points, Administration Server, or Kaspersky update servers, if this option is disabled.

  If you use distribution points to deploy installation packages, you can save traffic because you reduce the number of downloads. Also, you can relieve the load on the Administration Server and relocate the load between the distribution points. You can Calculating the number and configuration of distribution points the number of distribution points for your network to optimize the traffic and load.

If you disable this option, the number of installation package downloads and load on the Administration Server may increase. By default, the option is enabled.

**Enabled**

In Kaspersky Security Center Linux, a distribution point can work as a push server for the devices managed through the mobile protocol and for the devices managed by Network Agent. For example, a push server must be enabled if you want to be able to force synchronization of KasperskyOS devices with Administration Server. A push server has the same scope of managed devices as the distribution point on which the push server is enabled. If you have several distribution points assigned for the same administration group, you can enable push server on each of the distribution points. In this case, Administration Server balances the load between the distribution points.

**Push server port**

The port number for the push server. You can specify number of any unoccupied port.

- In the **Scope** section, specify administration groups to which the distribution point will distribute updates.
- In the **Source of updates** section, you can select a source of updates for the distribution point:

  **Source of updates**

  Select an update source for the distribution point:

  - To allow the distribution point to receive updates from the Administration Server, select **Retrieve from Administration Server**.
  - To allow the distribution point to receive updates by using a task, select **Use update download task**, and then specify a *Download updates to the repositories of distribution points* task:
    - If such a task already exists on the device, select the task in the list.
    - If no such task yet exists on the device, click the **Create task** link to create a task. The New task wizard starts. Follow the steps of the wizard.

  **Download diff files**

  This option enables the downloading diff files feature.

  By default, the option is enabled.

- If your distribution points use proxy server when connecting to the internet, in the **Internet connection settings** subsection, you can specify the following settings:

  **Use proxy server**

  If this check box is selected, an internet proxy server is used to connect distribution points to Kaspersky update servers. In the entry fields you can configure the proxy server connection.

  This check box is cleared by default.

  **Proxy server address**

  Address of the proxy server.

  **Port number**

  Port number that is used for connection.

  **Bypass proxy server for local addresses**

  If this option is enabled, no proxy server is used to connect to devices on the local network.

By default, this option is disabled.

**Proxy server authentication**

If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

This check box is cleared by default.

**User name**

User account under which connection to the proxy server is established.

**Password**

Password of the account under which the task will be run.

- In the **KSN Proxy** section, you can configure the application to use the distribution point to forward KSN requests from the managed devices:

  **Enable KSN Proxy on the distribution point side**

  The KSN proxy service is run on the device that is used as a distribution point. Use this feature to redistribute and optimize traffic on the network.

  The distribution point sends the KSN statistics, which are listed in the Kaspersky Security Network statement, to Kaspersky.

  By default, this option is disabled. Enabling this option takes effect only if the **Use Administration Server as a proxy server** and **I agree to use Kaspersky Security Network** options are enabled in the Administration Server properties window.

  You can assign a node of an active-passive cluster to a distribution point and enable KSN proxy server on this node.

  **Forward KSN requests to Administration Server**

  The distribution point forwards KSN requests from the managed devices to the Administration Server.

  By default, the option is enabled.

  **Access KSN Cloud/KPSN directly over the internet**

  The distribution point forwards KSN requests from managed devices to the KSN Cloud or KPSN. The KSN requests generated on the distribution point itself are also sent directly to the KSN Cloud or KPSN.

  **Ignore proxy server settings when connecting to KPSN**

  Enable this option, if you have the proxy server settings configured in the distribution point properties or in the Network Agent policy, but your network architecture requires that you use KPSN directly. Otherwise, requests from the managed applications cannot reach KPSN.

  This option is available if you select the **Access KSN Cloud/KPSN directly over the internet** option.

  **Port**

  The number of the TCP port that the managed devices will use to connect to KSN proxy server. The default port number is 13111.

  **Use UDP port**

  If you need the managed devices to connect to KSN proxy server through a UDP port, enable the **Use UDP port** option and specify a UDP port number. By default, the option is enabled.

  **UDP port**

The number of the UDP port that the managed devices will use to connect to KSN proxy server. The default UDP port to connect to the KSN proxy server is 15111.

**Use HTTPS**

If you need the managed devices to connect to KSN proxy server through an HTTPS port, enable the **Use HTTPS** option and specify an **HTTPS through port** number. The default HTTPS port to connect to the KSN proxy server is 17111.

**HTTPS port**

The number of the HTTPS port that the managed devices will use to connect to KSN proxy server. The default HTTPS port to connect to the KSN proxy server is 17111.

- In the **Connection gateway** section, you can configure the distribution point to act as a gateway for connection between Network Agent instances and Administration Server:

  **Connection gateway**

  If a direct connection between Administration Server and Network Agents cannot be established due to organization of your network, you can use the distribution point to act as the connection gateway between Administration Server and Network Agents.

  Enable this option if you need the distribution point to act as a connection gateway between Network Agents and Administration Server. By default, this option is disabled.

  **Establish connection to gateway from Administration Server (if gateway is in DMZ)**

  If Administration Server is located outside the demilitarized zone (DMZ), on local area network, Network Agents installed on remote devices cannot connect to Administration Server. You can use a distribution point as the connection gateway with reverse connectivity (Administration Server establishes a connection to distribution point).

  Enable this option if you need to connect Administration Server to the connection gateway in DMZ.

  **Open local port for Kaspersky Security Center Web Console**

  Enable this option if you need the connection gateway in DMZ to open a port for Web Console that is in DMZ or on the internet. Specify the port number that will be used for the connection from Web Console to the distribution point. The default port number is 13299.

  This option is available if you enable the **Establish connection to gateway from Administration Server (if gateway is in DMZ)** option.

  When connecting mobile devices to Administration Server via the distribution point that acts as a connection gateway, you can enable the following options:

  **Open port for mobile devices (SSL authentication of the Administration Server only)**

  Enable this option if you need the connection gateway to open a port for mobile devices and specify the port number that mobile devices will use for connection to distribution point. The default port number is 13292. The mobile device will check the Administration Server certificate. When establishing the connection, only Administration Server is authenticated.

  **Open port for mobile devices (two-way SSL authentication)**

Enable this option if you need connection gateway to open a port that will be used for two-way authentication of Administration Server and mobile devices. Mobile device will check the Administration Server certificate, and Administration Server will check the mobile device certificate. Specify the following settings:

- Port number that mobile devices will use for connection to the distribution point. The default port number is 13293.
- DNS domain names of the connection gateway that will be used by mobile devices. Separate domain names with commas. The specified domain names will be included in the distribution point certificate. If the domain names used by mobile devices do not match the common name in the distribution point certificate, mobile devices do not connect to the distribution point.

  The default DNS domain name is the FQDN name of the connection gateway.

In both cases, the certificates are checked during the TLS session establishment on distribution point only. The certificates are not forwarded to be checked by the Administration Server. After a TLS session with the mobile device is established, the distribution point uses the Administration Server certificate to create a tunnel for synchronization between the mobile device and Administration Server. If you open the port for two-way SSL authentication, the only way to distribute the mobile device certificate is via an installation package.

- Configure Windows network polling by the Windows-based distribution point.

  **Windows domains**

  You can enable device discovery for Windows domains and set the schedule for the discovery.

- Configure domain controller polling by the distribution point.

  **Domain controller polling**

  You can enable device discovery for domain controllers.

  In the **Polling** field, after you switch the toggle button to the **Enabled** position, you can select domain controllers for polling and also specify the polling schedule for them.

  If you use a Linux distribution point, in the **Poll specified domains** section, click **Add**, and then specify the address and user credentials of the domain controller. Also, you can specify the type of domain to be polled: Active Directory or Samba, FreeIPA, ALD Pro.

  If you use a Windows distribution point, you can select one of the following options:

  - **Poll current domain**
  - **Poll entire domain forest**
  - **Poll specified domains**

- Configure the polling of IP ranges by the distribution point.

  **IP ranges polling**

  You can enable device discovery for IPv4 ranges and IPv6 networks.

  If you enable the **Enable range polling** option, you can add scanned ranges and set the schedule for them. You can add IP ranges to the list of scanned ranges.

If you enable the **Use Zeroconf to poll IPv6 networks** option, the distribution point automatically polls the IPv6 network by using zero-configuration networking (also referred to as *Zeroconf*). In this case, the specified IP ranges are ignored because the distribution point polls the whole network. The **Use Zeroconf to poll IPv6 networks** option is available if the distribution point runs Linux. To use Zeroconf IPv6 polling, you must install the avahi-browse utility on the distribution point.

- In the **Advanced** section, specify the folder that the distribution point must use to store distributed data.

  **Use default folder**

  If you select this option, the application uses the Network Agent installation folder on the distribution point.

  **Use specified folder**

  If you select this option, in the field below, you can specify the path to the folder. It can be a local folder on the distribution point, or it can be a folder on any device on the corporate network.

  The user account used on the distribution point to run Network Agent must have read/write access to the specified folder.

10. Click **OK**.

    The selected devices act as distribution points.

# Adding a connection gateway in the DMZ as a distribution point

If Administration Server is outside the demilitarized zone (DMZ), Network Agents installed on external devices cannot connect to the Administration Server. In this case, you can use a distribution point as the connection gateway in DMZ. The distribution point opens a port for Administration Server to create the connection. When the Administration Server is started, it connects to that distribution point and maintains this connection during the entire session.

If you need to establish connection between Administration Server and your managed devices outside the period of synchronization between Network Agent and Administration Server, you have to enable a push server and open port 13295 on the Distribution point side.

We recommend that you use a specially assigned device as the connection gateway. For information about the maximum number of client devices (including mobile devices), refer to sizing guide.

A connection gateway waits for connections from Administration Server, rather than establishes connections to Administration Server. It means that right after a connection gateway is installed on a device in the DMZ, Administration Server does not list the device among managed devices. Therefore, you need a special procedure to ensure that Administration Server initiates a connection to the connection gateway.

*To add a device with a connection gateway as a distribution point:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Distribution points** section.

3. Select the **Manually assign distribution points** option.

4. In the toolbar, click the **Assign** button.

5. In the right pane that opens, do the following:

   a. Select the **Use DMZ connection gateway by address** option.

   b. In the **Connection gateway address** field, specify the device IP address or DNS name.

   c. Click the **Assign** button.

   d. The pane is closed, and the distribution point is displayed with the **Temporary entry for connection gateway** name.

6. Click the **Save** button.

   Administration Server attempts to connect to the connection gateway at the address that you specified. If it succeeds, the entry name changes to the name of the connection gateway device. This process takes up to five minutes.

If you open the distribution point properties by clicking the **Temporary entry for connection gateway** name, all options are grayed out. You can only view the General tab that displays the distribution point name. By default, port (13000) is used. You can configure the distribution point only after Administration Server connects to it. While the temporary entry for the connection gateway is being converted to a named entry, the connection gateway also appears in the Unassigned devices group.

*To add a connection gateway to a previously configured network:*

1. Install the Network Agent in the connection gateway mode.

2. Reinstall the Network Agent on devices that you want to connect to the newly added connection gateway.

# Modifying the list of distribution points for an administration group

You can view the list of distribution points assigned to a specific administration group and modify the list by adding or removing distribution points.

*To view and modify the list of distribution points assigned to an administration group:*

1. In the main menu, go to **Asset management** → **Managed devices**.

2. Select an administration group for which you want to view the assigned distribution points by clicking the **Show hierarchy** button at the top of the page, and then in the window that opens, click the name of the required group.

   This enables the **Distribution points** menu item.

   The path to the selected group is displayed at the top of the page. If necessary, in this path you can click a link with the administration group name to go to the group. By default, the last link in the path is inactive.

3. In the main menu, go to **Asset management** → **Distribution points**.

4. To add new distribution points for the administration group, click the **Assign** button.

5. To remove the assigned distribution points, select devices from the list and click the **Unassign** button.

Depending on your modifications, the new distribution points are added to the list or existing distribution points are removed from the list.

# Enabling a push server

In Kaspersky Security Center Linux, a distribution point can work as a push server for the devices managed through the mobile protocol and for the devices managed by Network Agent. For example, a push server must be enabled if you want to be able to force synchronization of KasperskyOS devices with Administration Server. A push server has the same scope of managed devices as the distribution point on which the push server is enabled. If you have several distribution points assigned for the same administration group, you can enable push server on each of the distribution points. In this case, Administration Server balances the load between the distribution points.

You might want to use distribution points as push servers to make sure that there is continuous connectivity between a managed device and the Administration Server. Continuous connectivity is needed for some operations, such as running and stopping local tasks, receiving statistics for a managed application, or creating a tunnel. If you use a distribution point as a push server, you do not have to use the **Do not disconnect from the Administration Server** option on managed devices or send packets to the UDP port of the Network Agent.

A push server supports the load of up to 50,000 simultaneous connections.

*To enable push server on a distribution point:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Distribution points** section.

3. Click the name of the distribution point on which you want to enable the push server.

   The distribution point properties window opens.

4. On the **General** section, enable the **Enabled** option.

5. In the **Push server port** field, type the port number. You can specify number of any unoccupied port.

6. In the **Address for remote hosts** field, specify the IP address or the name of the distribution point device.

7. Click **OK**.

The push server is enabled on the selected distribution point.

# Increasing the limit of file descriptors for the klnagent service

If the scope of a Linux-based distribution point includes many devices, the default limit of files that can be opened (file descriptors) may not be enough. To avoid this, you can increase the limit of file descriptors for the klnagent service.

*To increase the limit of file descriptors for the klnagent service:*

1. On the Linux-based device that acts as a distribution point, execute the following command:

   ```
   systemctl edit klnagent64.service
   ```

2. Specify the hard and soft limits of the file descriptors in the `LimitNOFILE` parameter of the `[Service]` section:

   `LimitNOFILE=<soft resource limit>:<hard resource limit>`

   For example, `LimitNOFILE=32768:131072`. Note that the soft limit of the file descriptors must be less or equal to the hard limit.

3. Run the following command to ensure that the parameters are specified correctly:

   ```
   systemd-analyze verify klnagent64.service
   ```

   If the parameters are specified incorrectly, this command can output one of the following errors:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     If this error occurs, the symbols in the `LimitNOFILE` line were specified incorrectly. You must check and correct the entered line.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     If this error occurs, the soft limit of the file descriptors you entered is more than the hard limit. You must check the entered line and ensure that the soft limit of the file descriptors is less or equal to the hard limit.

4. Run the following command to reload the systemd process:

   ```
   systemctl daemon-reload
   ```

5. Run the following command to restart the Network Agent service:

   ```
   systemctl restart klnagent
   ```

6. Run the following command to ensure that the specified parameters are applied correctly:

   `less /proc/<nagent process id>/limits`

   where the `<nagent process id>` parameter is the identifier of the Network Agent process. You can run the following command to obtain the identifier:

   ```
   ps -ax | grep klnagent
   ```

For the Linux-based distribution point, the limit of files that can be opened is increased.

# About device statuses

Kaspersky Security Center Linux assigns a status to each managed device. The particular status depends on whether the conditions defined by the user are met. In some cases, when assigning a status to a device, Kaspersky Security Center Linux takes into consideration the device's visibility flag on the network (see the table below). For example, if a managed device was assigned the *Critical* status because the *Databases are outdated* condition was met, and later the visibility flag was set for the device, then the device is assigned the *OK* status. If Kaspersky Security Center Linux does not find a device on the network within two hours, the visibility flag of the device is set to *Not Visible*.

The statuses are the following:

- *Critical* or *Critical/Visible*
- *Warning* or *Warning/Visible*
- *OK* or *OK/Visible*

The table below lists the default conditions that must be met to assign the *Critical* or *Warning* status to a device, with all possible values.

Conditions for assigning a status to a device

| Condition | Condition description | Available values |
|---|---|---|
| Security application is not installed | Network Agent is installed on the device, but a security application is not installed. | • Toggle button is on<br>• Toggle button is off |
| Too many viruses detected | Some viruses have been found on the device by a task for virus detection, for example, the Malware scan task, and the number of viruses found exceeds the specified value. | More than 0 |
| Real-time protection level differs from the level set by the Administrator | The device is visible on the network, but the real-time protection level differs from the level set (in the condition) by the administrator for the device status. | • Stopped<br>• Suspended<br>• Running |
| Malware scan has not been performed in a long time | The device is visible on the network and a security application is installed on the device, but neither the *Malware scan* task nor a local scan task has been run within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 7 days ago or earlier. | More than 1 day |
| Databases are outdated | The device is visible on the network and a security application is installed on the device, but the anti-virus databases have not been updated on this device within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 1 day ago or earlier. | More than 1 day |
| Not connected in a long time | Network Agent is installed on the device, but the device has not connected to an Administration Server within the specified time interval, because the device was turned off. | More than 1 day |
| Active threats are detected | The number of unprocessed objects in the **Active threats** folder exceeds the specified value. | More than 0 items |

| Condition | Condition description | Available values |
|---|---|---|
| Time since restart required | The device is visible on the network, but a restart has been required by an application for longer than the specified time interval. | More than 0 minutes |
| Restart reason | The device is visible on the network, but an application requires a device restart for one of the selected reasons. | • Unknown reason<br>• Application will not run until restart<br>• Restart is required to complete update; application is running<br>• Restart is required to launch update<br>• Restart is required to complete scan or disinfection<br>• Restart is required to complete remote installation/uninstallation<br>• Completing data encryption on disk |
| Incompatible applications are installed | The device is visible on the network, but software inventory performed through Network Agent has detected incompatible applications installed on the device. | • Toggle button is off<br>• Toggle button is on |
| Software vulnerabilities have been detected | The device is visible on the network and Network Agent is installed on the device, but the *Find vulnerabilities and required updates* task has detected vulnerabilities with the specified severity level in applications installed on the device. | • Critical<br>• High<br>• Medium<br>• Ignore if the vulnerability cannot be fixed<br>• Ignore if an update is assigned for installation |
| License expired | The device is visible on the network, but the license has expired. | • Toggle button is off<br>• Toggle button is on |
| License expires soon | The device is visible on the network, but the license will expire on the device in less than the specified number of days. | More than 0 days. |
| Check for Windows Update updates has not been performed in a long time | The device is visible on the network, but the *Find vulnerabilities and required updates* task has not been run within the specified time interval. | More than 1 day |
| Invalid encryption status | Network Agent is installed on the device, but the device encryption result is equal to the specified value. | • Does not comply with the policy due to the user's refusal (for external devices only)<br>• Does not comply with the policy due to an error<br>• Restart is required when applying the policy<br>• No encryption policy is specified<br>• Not supported<br>• When applying the policy |
| Mobile device settings do not comply with the policy | The mobile device settings are other than the settings that were specified in the Kaspersky Endpoint Security for Android policy during the check of compliance rules. | • Toggle button is off<br>• Toggle button is on |
| Unprocessed security issues detected | Some unprocessed security issues have been found on the device. Security issues can be created either automatically, through managed Kaspersky applications installed on the client device, or manually by the administrator. | • Toggle button is off<br>• Toggle button is on |
| Device status defined by application | The status of the device is defined by the managed application.<br>Managed devices can have a status defined by managed applications regardless of Kaspersky Security Center Linux settings. After this status returns one of the statuses defined by Kaspersky Security Center Linux, Administration Server assigns to a managed device the most critical status of those returned by the managed application and assigned by Administration Server. Statuses defined by managed applications have descriptions transferred by managed applications. You can view the descriptions in the list of managed devices, **Status description** column. | • Toggle button is off<br>• Toggle button is on |

| Condition | Condition description | Available values |
|---|---|---|
| Device is out of disk space | Free disk space on the device is less than the specified value, or the device could not be synchronized with the Administration Server. The *Critical* or *Warning* status is changed to the *OK* status when the device is successfully synchronized with the Administration Server and free space on the device is greater than or equal to the specified value. | More than 0 MB |
| Device has become unmanaged | During device discovery, the device was recognized as visible on the network, but more than three attempts to synchronize with the Administration Server failed. | • Toggle button is off<br>• Toggle button is on |
| Protection is disabled | The device is visible on the network, but the security application on the device has been disabled for longer than the specified time interval.<br>In this case, the state of the security application is *stopped* or *failure*, and differs from the following: *starting*, *running*, or *suspended*. | More than 0 minutes |
| Security application is not running | The device is visible on the network and a security application is installed on the device but is not running. | • Toggle button is off<br>• Toggle button is on |

Kaspersky Security Center Linux allows you to set up automatic switching of the status of a device in an administration group when specified conditions are met. When the specified conditions are met, the client device is assigned one of the following statuses: *Critical* or *Warning*. When the specified conditions are not met, the client device is assigned the *OK* status.

Different statuses may correspond to different values of one condition. For example, by default, if the **Databases are outdated** condition has the **More than 3 days** value, the client device is assigned the *Warning* status; if the value is **More than 7 days**, the *Critical* status is assigned.

If you upgrade Kaspersky Security Center Linux from the previous version, the values of the **Databases are outdated** condition for assigning the status to *Critical* or *Warning* do not change.

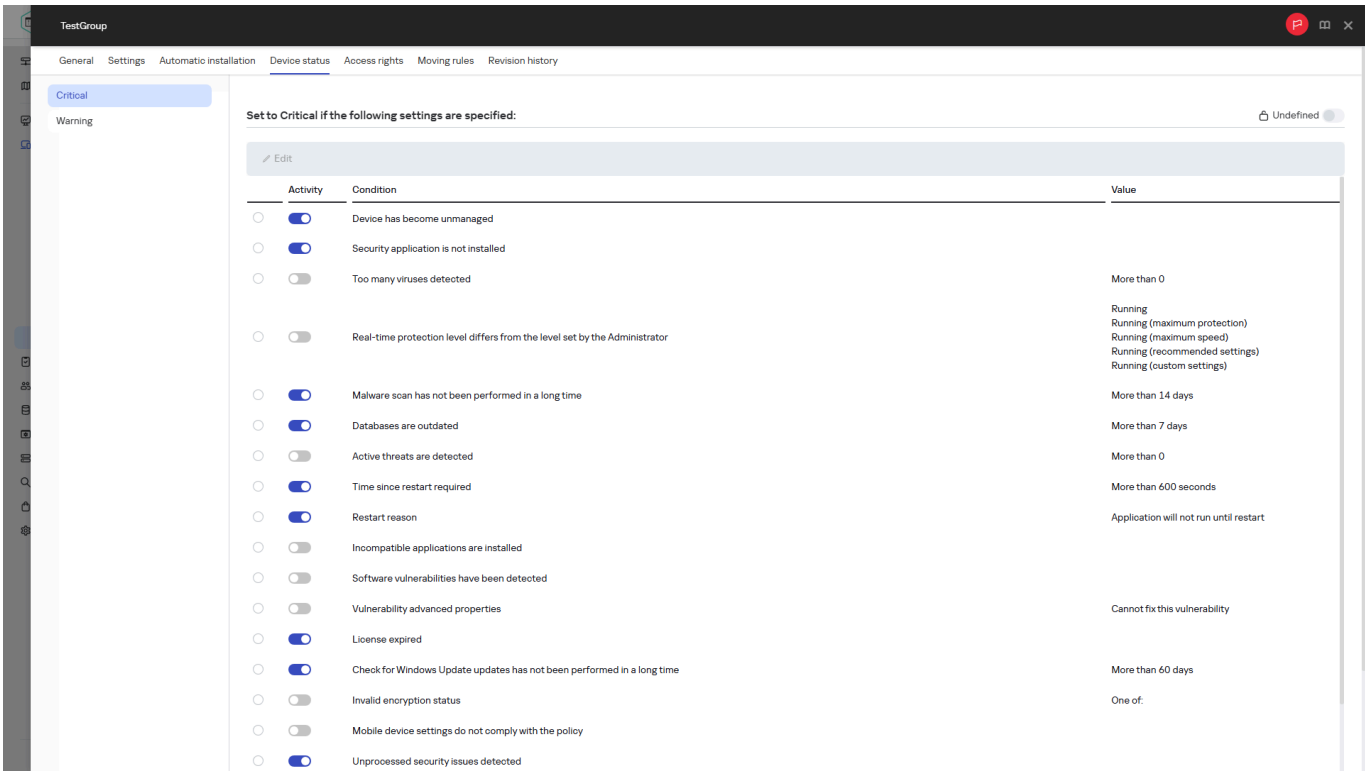
# Configuring the switching of device statuses

You can change conditions to assign the *Critical* or *Warning* status to a device.

*To enable changing the device status to Critical:*

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. Go to the properties of the administration group for which you want to change the device statuses in one of the following ways:
   - Click the name of the administration group.
   - Click the **Show hierarchy** button at the top of the page. In the navigation pane that opens, hover the mouse cursor over the name of the required group, and then click the settings icon ( ⚙ ).

   The administration group properties window opens.
3. In the properties window, select the **Device status** tab.
4. In the left pane, select **Critical**.
5. In the right pane, in the **Set to Critical if the following settings are specified** section, enable the condition to switch a device to the *Critical* status.




You can change only settings that are not locked in the parent policy.

6. Select the radio button next to the condition in the list.
7. In the upper-left corner of the list, click the **Edit** button.
8. Set the required value for the selected condition.

   Values cannot be set for every condition.
9. Click **OK**.
10. Click **Save** to save changes.

When specified conditions are met, the managed device is assigned the *Critical* status.

*To enable changing the device status to Warning:*

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. In the list of groups that opens, click the link with the name of a group for which you want to change switching the device statuses.
3. In the properties window that opens, select the **Device status** tab.
4. In the left pane, select **Warning**.
5. In the right pane, in the **Set to Warning if the following settings are specified** section, enable the condition to switch a device to the *Warning* status.

You can change only settings that are not locked in the parent policy.

6. Select the radio button next to the condition in the list.
7. In the upper-left corner of the list, click the **Edit** button.
8. Set the required value for the selected condition.

   Values cannot be set for every condition.
9. Click **OK**.
10. Click **Save** to save changes.

When specified conditions are met, the managed device is assigned the *Warning* status.

# Device selections

*Device selections* are a tool for filtering devices according to specific conditions. You can use device selections to manage several devices: for example, to view a report about only these devices or to move all of these devices to another group.

Kaspersky Security Center Linux provides a broad range of *predefined selections* (for example, **Devices with Critical status**, **Protection is disabled**, **Active threats are detected**). Predefined selections cannot be deleted. You can also create and configure additional *user-defined selections*.

In user-defined selections, you can set the search scope and select all devices, managed devices, or unassigned devices. Search parameters are specified in the conditions. In the device selection you can create several conditions with different search parameters. For example, you can create two conditions and specify different IP ranges in each of them. If several conditions are specified, a selection displays the devices that meet any of the conditions. By contrast, search parameters within a condition are superimposed. If both an IP range and the name of an installed application are specified in a condition, only those devices will be displayed where both the application is installed and the IP address belongs to the specified range.

## Viewing the device list from a device selection

Kaspersky Security Center Linux allows you to view the list of devices from a device selection.

*To view the device list from the device selection:*

1. In the main menu, go to the **Asset management** → **Device selections** or **Discovery & deployment** → **Device selections** section.
2. In the selection list, click the name of the device selection.

   The page displays a table with information about the devices included in the device selection.
3. You can group and filter the data of the device table as follows:

   - Click the settings icon (⚙), and then select the columns to be displayed in the table.
   - Click the filter icon ( ▽ ), and then specify and apply the filter criterion in the invoked menu.

     The filtered table of devices is displayed.

You can also run tasks for device selections. To do this, select one or more devices, then click the **Run task** button and select: **Create task** to be applied to these devices, or **Use existing task**.

To move the selected devices of the device selection to another administration group, click the **Move to group** button, and then select the target administration group.

# Creating a device selection

*To create a device selection:*

1. In the main menu, go to **Asset management** → **Device selections**.

   A page with a list of device selections is displayed.

2. Click the **Add** button.

   The **Device selection settings** window opens.

3. Enter the name of the new selection.

4. Specify the group that contains the devices to be included in the device selection:

   - **Find any devices**—Searching for devices that meet the selection criteria and included in the **Managed Devices** or **Unassigned devices** group.
   - **Find managed devices**—Searching for devices that meet the selection criteria and included in the **Managed Devices** group.
   - **Find unassigned devices**—Searching for devices that meet the selection criteria and included in the **Unassigned devices** group.

   You can enable the **Include data from secondary Administration Servers** check box to enable searching for devices that meet the selection criteria and managed by secondary Administration Servers.

5. Click the **Add** button.

6. In the window that opens, specify conditions that must be met for including devices in this selection, and then click the **Save** button.

7. Click the **Save** button.

The device selection is created and added to the list of device selections.

# Configuring a device selection

*To configure a device selection:*

1. In the main menu, go to **Asset management** → **Device selections**.

   A page with a list of device selections is displayed.

2. Select the relevant user-defined device selection, and click the **Properties** button.

   The **Device selection settings** window opens.

3. On the **General** tab, click the **New condition** link.

4. Specify conditions that must be met for including devices in this selection.

5. Click the **Save** button.

   The settings are applied and saved.

Below are descriptions of the conditions for assigning devices to a selection. Conditions are combined by using the OR logical operator: the selection will contain devices that comply with at least one of the listed conditions.

### General

In the **General** section, you can change the name of the selection condition and specify whether that condition must be inverted:

**Invert selection condition**

By default, this option is disabled.

If you enable this option, the specified selection condition will be inverted. The selection will include all devices that do not meet the condition.

The following example shows the logic of the inversion work:

- **Condition**: On your device, there is an operating system with the Linux type and the 00.0.000 build number.
- **Inverted condition**: On your device, there is an operating system with NOT (the Linux type and the 00.0.000 build number), which is equivalent to the following:

  There is an operating system with the type NOT Linux OR build number NOT 00.0.000.

Thus, the selection will include the devices with an operating system, for example, of the Windows type and the 00.0.000 build number, or the Linux type and any build number other than 00.0.000.

### Network infrastructure

In the **Network** subsection, you can specify the criteria that will be used to include devices in the selection according to their network data:

**Device name**

Windows network name (NetBIOS name) of the device, or the IPv4 or IPv6 address.

**Domain**

Displays all devices included in the specified workgroup.

**Administration group**

Displays devices included in the specified administration group.

**Description**

Text in the device properties window: in the **Description** field of the **General** section.

To describe text in the **Description** field, you can use the following characters:

- Within a word:
  - *****. Replaces any string with any number of characters.

  **Example**:

  To describe words such as **Server** or **Server's**, you can enter **Server***.

  - **?.** Replaces any single character.

  **Example**:

  To describe phrases such as **SUSE Linux Enterprise Server 12** or **SUSE Linux Enterprise Server 15**, you can enter **SUSE Linux Enterprise Server 1?**.

  Asterisk (*****) or question mark (**?**) cannot be used as the first character in the query.

- To find several words:
  - Space. Displays all the devices whose descriptions contain any of the listed words.

  **Example**:

  To find a phrase that contains **Secondary** or **Virtual** words, you can include **Secondary Virtual** line in your query.

  - **+**. When a plus sign precedes a word, all search results will contain this word.

  **Example**:

  To find a phrase that contains both **Secondary** and **Virtual**, enter the **+Secondary+Virtual** query.

  - **-**. When a minus sign precedes a word, no search results will contain this word.

  **Example**:

  To find a phrase that contains **Secondary** and does not contain **Virtual**, enter the **+Secondary-Virtual** query.

  - **"<some text>"**. Text enclosed in quotation marks must be present in the text.

  **Example**:

  To find a phrase that contains **Secondary Server** word combination, you can enter **"Secondary Server"** in the query.

**IP range**

If this option is enabled, you can enter the initial and final IP addresses of the IP range in which the relevant devices must be included.

By default, this option is disabled.

**Managed by a different Administration Server**

Select one of the following values:

- **Yes**. A device moving rule only applies to client devices managed by other Administration Servers. These Servers are different from the Server on which you configure the device moving rule.
- **No**. The device moving rule only applies to client devices managed by the current Administration Server.
- **No value is selected**. The condition does not apply.

In the **Domain controller** subsection, you can configure criteria for including devices into a selection based on domain membership:

**Device is in a domain organizational unit**

If this option is enabled, the selection includes devices from the domain organizational unit specified in the entry field.

By default, this option is disabled.

**This device is a member of the domain security group**

If this option is enabled, the selection includes devices from the domain security group specified in the entry field.

By default, this option is disabled.

In the **Network activity** subsection, you can specify the criteria that will be used to include devices in the selection according to their network activity:

**Acts as a distribution point**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes**. The selection includes devices that act as distribution points.
- **No**. Devices that act as distribution points are not included in the selection.
- **No value is selected**. The criterion will not be applied.

**Do not disconnect from the Administration Server**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Enabled**. The selection will include devices on which the **Do not disconnect from the Administration Server** check box is selected.
- **Disabled**. The selection will include devices on which the **Do not disconnect from the Administration Server** check box is cleared.
- **No value is selected**. The criterion will not be applied.

**Connection profile switched**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes**. The selection will include devices that connected to the Administration Server after the connection profile was switched.
- **No**. The selection will not include devices that connected to the Administration Server after the connection profile was switched.
- **No value is selected**. The criterion will not be applied.

**Last connected to Administration Server**

You can use this check box to set a search criterion for devices according to the time they last connected to the Administration Server.

If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last connection was established between Network Agent installed on the client device and the Administration Server. The selection will include devices that fall within the specified interval.

If this check box is cleared, the criterion will not be applied.

This check box is cleared by default.

**New devices detected by network poll**

Searches for new devices that have been detected by network polling over the last few days.

If this option is enabled, the selection only includes new devices that have been detected by device discovery over the number of days specified in the **Detection period (days)** field.

If this option is disabled, the selection includes all devices that have been detected by device discovery.

By default, this option is disabled.

**Device is visible**

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes**. The application includes in the selection devices that are currently visible in the network.
- **No**. The application includes in the selection devices that are currently invisible in the network.
- **No value is selected**. The criterion will not be applied.

### Device statuses

In the **Managed device status** subsection, you can configure criteria for including devices into a selection based on the description of the devices status from a managed application:

**Device status**

Drop-down list in which you can select one of the device statuses: *OK*, *Critical*, or *Warning*.

**Real-time protection status**

Drop-down list, in which you can select the real-time protection status. Devices with the specified real-time protection status are included in the selection.

**Device status description**

In this field, you can select the check boxes next to conditions that, if met, assign one of the following statuses to the device: *OK, Critical*, or *Warning*.

In the **Status of components in managed applications** subsection, you can configure criteria for including devices in a selection according to the statuses of components in managed applications:

**Data Leakage Prevention status**

Search for devices by the status of Data Leakage Prevention (*Unknown, Stopped, Starting, Paused, Running, Failed*).

**Collaboration servers protection status**

Search for devices by the status of server collaboration protection (*Unknown*, *Stopped*, *Starting*, *Paused*, *Running*, *Failed*).

**Anti-virus protection status of mail servers**

Search for devices by the status of Mail Server protection (*Unknown, Stopped, Starting, Paused, Running, Failed*).

**Endpoint Sensor status**

Search for devices by the status of the Endpoint Sensor component (*Unknown, Stopped, Starting, Paused, Running, Failed*).

In the **Status-affecting problems in managed applications** subsection, you can specify the criteria that will be used to include devices in the selection according to the list of possible problems detected by a managed application. If at least one problem that you select exists on a device, the device will be included in the selection. When you select a problem listed for several applications, you have the option to select this problem in all of the lists automatically.

You can select check boxes for descriptions of statuses from the managed application; upon receipt of these statuses, the devices will be included in the selection. When you select a status listed for several applications, you have the option to select this status in all of the lists automatically.

### System details

In the **OS** section, you can specify the criteria that will be used to include devices in the selection according to their operating system type.

**Platform type**

If the check box is selected, you can select an operating system from the list. Devices with the specified operating systems installed are included in the search results.

**OS service pack version**

In this field, you can specify the package version of the operating system (in the *X.Y* format), which will determine how the moving rule is applied to the device. By default, no version value is specified.

**OS architecture**

In the drop-down list, you can select the architecture for the operating system, which will determine how the moving rule is applied to the device (**Unknown**, **x86**, **AMD64**, or **IA64**). By default, no option is selected in the list so that the operating system's architecture is not defined.

**OS build**

This setting is applicable to Windows operating systems only.

The build number of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later release number. You can also configure searching for all build numbers except the specified one.

**OS release number**

> This setting is applicable to Windows operating systems only.

The release identifier (ID) of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later release ID. You can also configure searching for all release ID numbers except the specified one.

In the **Virtual machines** section, you can set up the criteria to include devices in the selection according to whether these are virtual machines or part of virtual desktop infrastructure (VDI):

**This is a virtual machine**

In the drop-down list, you can select the following options:

- **Undefined**.
- **No**. Find devices that are not virtual machines.
- **Yes**. Find devices that are virtual machines.

**Virtual machine type**

In the drop-down list, you can select the virtual machine manufacturer.

This drop-down list is available if the **Yes** or **Not important** value is selected in the **This is a virtual machine** drop-down list.

**Part of Virtual Desktop Infrastructure**

In the drop-down list, you can select the following options:

- **Undefined**.
- **No**. Find devices that are not part of Virtual Desktop Infrastructure.
- **Yes**. Find devices that are part of the Virtual Desktop Infrastructure (VDI).

In the **Hardware registry** subsection, you can configure criteria for including devices into a selection based on their installed hardware:

> Ensure that the lshw utility is installed on Linux devices from which you want to fetch hardware details. Hardware details fetched from virtual machines may be incomplete depending on the hypervisor used.

**Device**

In the drop-down list, you can select a unit type. All devices with this unit are included in the search results.

The field supports the full-text search.

**Vendor**

In the drop-down list, you can select the name of a unit manufacturer. All devices with this unit are included in the search results.

The field supports the full-text search.

**Device name**

The device with the specified name is included in the selection.

**Description**

Description of the device or hardware unit. Devices with the description specified in this field are included in the selection.

A device's description in any format can be entered in the properties window of that device. The field supports the full-text search.

**Device vendor**

Name of the device manufacturer. Devices produced by the manufacturer specified in this field are included in the selection.

You can enter the manufacturer's name in the properties window of a device.

**Serial number**

All hardware units with the serial number specified in this field will be included in the selection.

**Inventory number**

Equipment with the inventory number specified in this field will be included in the selection.

**User**

All hardware units of the user specified in this field will be included in the selection.

**Location**

Location of the device or hardware unit (for example, at the HQ or a branch office). Computers or other devices that are deployed at the location specified in this field will be included in the selection.

You can describe the location of a device in any format in the properties window of that device.

**CPU clock rate, in MHz, from**

The minimum clock rate of a CPU. Devices with a CPU that matches the clock rate range specified in the entry fields (inclusive) will be included in the selection.

**CPU clock rate, in MHz, to**

The maximum clock rate of a CPU. Devices with a CPU that matches the clock rate range specified in the entry fields (inclusive) will be included in the selection.

**Number of virtual CPU cores, from**

The minimum number of virtual CPU cores. Devices with a CPU that matches the range of the virtual cores number specified in the entry fields (inclusive) will be included in the selection.

**Number of virtual CPU cores, to**

The maximum number of virtual CPU cores. Devices with a CPU that matches the range of the virtual cores number specified in the entry fields (inclusive) will be included in the selection.

**Hard drive volume, in GB, from**

The minimum volume of the hard drive on the device. Devices with a hard drive that matches the volume range specified in the entry fields (inclusive) will be included in the selection.

**Hard drive volume, in GB, to**

The maximum volume of the hard drive on the device. Devices with a hard drive that matches the volume range specified in the entry fields (inclusive) will be included in the selection.

**RAM size, in MB, from**

The minimum size of the device RAM. Devices with RAM that matches the range of values in the entry fields (inclusive) are included in the selection.

**RAM size, in MB, to**

The maximum size of the device RAM. Devices with RAM that matches the size range specified in the entry fields (inclusive) will be included in the selection.

### Third-party software details

In the **Applications registry** subsection, you can set up the criteria to search for devices according to applications installed on them:

**Application name**

Drop-down list in which you can select an application. Devices on which the specified application is installed, are included in the selection.

**Application version**

Entry field in which you can specify the version of selected application.

**Vendor**

Drop-down list in which you can select the manufacturer of an application installed on the device.

**Application status**

A drop-down list in which you can select the status of an application (*Installed*, *Not installed*). Devices on which the specified application is installed or not installed, depending on the selected status, will be included in the selection.

**Find by update**

If this option is enabled, search will be performed using the details of updates for applications installed on the relevant devices. After you select the check box, the **Application name**, **Application version**, and **Application status** fields change to **Update name**, **Update version**, and **Status** respectively.

By default, this option is disabled.

**Name of incompatible security application**

Drop-down list in which you can select third-party security applications. During the search, devices on which the specified application is installed, are included in the selection.

**Application tag**

In the drop-down list, you can select the application tag. All devices that have installed applications with the selected tag in the description are included in the device selection.

**Apply to devices without the specified tags**

If this option is enabled, the selection includes devices with descriptions that contain none of the selected tags.

If this option is disabled, the criterion is not applied.

By default, this option is disabled.

In the **Vulnerabilities and updates** subsection, you can specify the criteria that will be used to include devices in the selection according to their Windows Update source:

**WUA is switched to Administration Server**

You can select one of the following search options from the drop-down list:

- **Yes**. If this option is selected, the search results will include devices that receive updates through Windows Update from the Administration Server.
- **No**. If this option is selected, the results will include devices that receive updates through Windows Update from another sources.

### Details of Kaspersky applications

In the **Kaspersky applications** subsection, you can configure criteria for including devices in a selection based on the selected managed application:

**Application name**

In the drop-down list, you can set a criterion for including devices in a selection when search is performed by the name of a Kaspersky application.

The list provides only the names of applications with management plug-ins installed on the administrator's workstation.

If no application is selected, the criterion will not be applied.

**Application version**

In the entry field, you can set a criterion for including devices in a selection when search is performed by the version number of a Kaspersky application.

If no version number is specified, the criterion will not be applied.

**Critical update name**

In the entry field, you can set a criterion for including devices in a selection when search is performed by application name or by update package number.

If the field is left blank, the criterion will not be applied.

**Application status**

A drop-down list in which you can select the status of an application (*Installed*, *Not installed*). Devices on which the specified application is installed or not installed, depending on the selected status, will be included in the selection.

**Select the period of the last update of modules**

You can use this option to set a criterion for searching devices by time of the last update of modules of applications installed on those devices.

If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last update of modules of applications installed on those devices was performed.

If this check box is cleared, the criterion will not be applied.

This check box is cleared by default.

**Device is managed through Administration Server**

In the drop-down list, you can include in the selection the devices managed through Kaspersky Security Center Linux:

- **Yes**. The application includes in the selection devices managed through Kaspersky Security Center Linux.
- **No**. The selection includes devices that are not managed by Kaspersky Security Center.
- **No value is selected**. The criterion will not be applied.

**Security application is installed**

In the drop-down list, you can include in the selection all devices with the security application installed:

- **Yes**. The application includes in the selection all devices with the security application installed.
- **No**. The application includes in the selection all devices with no security application installed.
- **No value is selected**. The criterion will not be applied.

In the **Anti-virus protection** subsection, you can set up the criteria for including devices in a selection based on their protection status:

**Databases released**

If this option is selected, you can search for client devices by anti-virus database release date. In the entry fields you can set the time interval, on the basis of which the search is performed.

By default, this option is disabled.

**Database records count**

If this option is enabled, you can search for client devices by number of database records. In the entry fields you can set the lower and upper threshold values for anti-virus database records.

By default, this option is disabled.

**Last scanned**

If this check option is enabled, you can search for client devices by time of the last malware scan. In the entry fields you can specify the time period within which the last malware scan was performed.

By default, this option is disabled.

**Threats detected**

If this option is enabled, you can search for client devices by number of viruses detected. In the entry fields you can set the lower and upper threshold values for the number of viruses found.

By default, this option is disabled.

In the **Encryption** subsection, you can configure the criterion for including devices in a selection based on the selected encryption algorithm:

#### Encryption algorithm

Advanced Encryption Standard (AES) symmetrical block cipher algorithm. In the drop-down list, you can select the encryption key size (56-bit, 128-bit, 192-bit, or 256-bit).

Available values: *AES56*, *AES128*, *AES192*, and *AES256*.

The **Application components** subsection contains the list of components of those applications that have corresponding management plug-ins installed in Kaspersky Security Center Web Console.

In the **Application components** subsection, you can specify criteria for including devices in a selection according to the statuses and version numbers of the components that refer to the application that you select:

#### Status

Search for devices according to the component status sent by an application to the Administration Server. You can select one of the following statuses: *N/A, Stopped*, *Paused*, *Starting*, *Running*, *Failed, Not installed, Not supported by license*. If the selected component of the application installed on a managed device has the specified status, the device is included in the device selection.

Statuses sent by applications:

- *Stopped*—The component is disabled and not working at the moment.
- *Paused*—The component is suspended, for example, after the user has paused protection in the managed application.
- *Starting*—The component is currently in the process of initialization.
- *Running*—The component is enabled and working properly.
- *Failed*—An error has occurred during the component operation.
- *Not installed*—The user did not select the component for installation when configuring custom installation of the application.
- *Not supported by license*—The license does not cover the selected component.

Unlike other statuses, the *N/A* status is not sent by applications. This option shows that the applications have no information about the selected component status. For example, this can happen when the selected component does not belong to any of the applications installed on the device, or when the device is turned off.

#### Version

Search for devices according to the version number of the component that you select in the list. You can type a version number, for example `3.4.1.0`, and then specify whether the selected component must have an equal, earlier, or later version. You can also configure searching for all versions except the specified one.

### Tags

In the **Tags** section, you can configure criteria for including devices into a selection based on key words (tags) that were previously added to the descriptions of managed devices:

#### Apply if at least one specified tag matches

If this option is enabled, the search results will show devices with descriptions that contain at least one of the selected tags.

If this option is disabled, the search results will only show devices with descriptions that contain all the selected tags.

By default, this option is disabled.

To add tags to the criterion, click the **Add** button, and select tags by clicking the **Tag** entry field. Specify whether to include or exclude the devices with the selected tags in the device selection.

#### All devices that have this tag

If this option is selected, the search results will display the devices whose descriptions contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

By default, this option is selected.

#### All devices that do not have this tag

If this option is selected, the search results will display the devices whose descriptions do not contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

### Users

In the **Users** section, you can set up the criteria to include devices in the selection according to the accounts of users who have logged in to the operating system.

#### Last user who logged in to the system

If this option is enabled, you can select the user account for configuring the criterion. The search results include devices on which the selected user performed the last login to the system.

#### User who logged in to the system at least once

If this option is enabled, click the **Browse** button to specify a user account. The search results include devices on which the specified user logged in to the system at least once.

### Device owner

In the **Device owner** section, you can set up the criteria to include devices in the selection according to the registered owners of the device, their roles, and their membership in security groups:

#### Device owner

Select a device owner's user name from an internal security group. Learn more about users and user roles in this section.

> No more than one user can be registered as the device owner.

**Device owner's membership in Active Directory security group**

Select an external Active Directory security group that the device owner belongs to.

> The user can be a part of an Active Directory security group or a part of a group that is included in this Active Directory security group.

**Device owner's role**

Select the device owner's assigned role. Learn more about user roles in this article.

**Device owner's membership in an internal security group**

Select an internal security group that the device owner belongs to.

### Custom parameters

> Custom settings are available only with the Kaspersky Mobile Devices Protection and Management plug-in 10.59.4.32 or later installed.

In the **Custom parameters** section, you can configure the criteria for including Android devices in the device selection based on the values of custom settings. For detailed information on using custom settings, refer to the Kaspersky Secure Mobility Management Help.

## Exporting the device list from a device selection

Kaspersky Security Center Linux allows you to save information about devices from a device selection and export it as a CSV or a TXT file.

*To export the device list from the device selection:*

1. Open the table with the devices from the device selection.
2. Use one of the following ways to select the devices that you want to export:
   - To select particular devices, select the check boxes next to them.
   - To select all devices from the current table page, select the check box in the device table header, and then select the **Select all on current page** check box.
   - To select all devices from the table, select the check box in the device table header, and then select the **Select all** check box.
3. Click the **Export to CSV** or **Export to TXT** button. All information about the selected devices included in the table will be exported.

Note that if you applied a filter criterion to the device table, only the filtered data from the displayed columns will be exported.

# Removing devices from administration groups in a selection

When working with a device selection, you can remove devices from administration groups right in this selection, without switching to the administration groups from which these devices must be removed.

*To remove devices from administration groups:*

1. In the main menu, go to **Asset management** → **Device selections** or **Discovery & deployment** → **Device selections**.
2. In the selection list, click the name of the device selection.

   The page displays a table with information about the devices included in the device selection.
3. Select the devices that you want to remove, and then click **Delete**.

   The selected devices are removed from their respective administration groups.

# Device tags

Kaspersky Security Center Linux allows you to *tag* devices. A tag is the string value that can be used for grouping, describing, or finding devices. Tags assigned to devices can be used for creating selections, for finding devices, and for distributing devices among administration groups.

You can tag devices manually or automatically. If you want to tag an individual device, you can use manual tagging. Auto-tagging is performed by Kaspersky Security Center Linux in one of the following ways:

- In accordance with the specified tagging rules.
- By an application.

> We do not recommend that you use different ways of tagging to assign the same tag. For example, if the tag is assigned by the rule, it is not recommended to manually assign this tag to devices.

If the tags are assigned by rules, devices are tagged automatically when the specified rules are met. An individual rule corresponds to each tag. Rules are applied to the network properties of the device, operating system, applications installed on the device, and other device properties. For example, you can set up a rule that will assign the `[CentOS]` tag to all devices running CentOS operating system. Then, you can use this tag when creating a device selection; this will help you sort all CentOS devices and assign them a task.

> You can add only one auto-tagging rule per tag. If you create a new rule for the same tag, the previous one will be replaced.

A tag is automatically removed from a device in the following cases:

- When the device stops meeting conditions of the rule that assigns the tag.
- When the rule that assigns the tag is disabled or deleted.

The list of tags and the list of rules on each Administration Server are independent of all other Administration Servers, including a primary Administration Server or subordinate virtual Administration Servers. A rule is applied only to devices from the same Administration Server on which the rule is created.

# Creating a device tag

*To create a device tag:*

1. In the main menu, go to **Repositories** → **Device tags**.
2. On the **Device tags** tab, click the **Add** button.

   A new tag window opens.
3. In the **Tag** field, enter the tag name.
4. Click **Save** to save changes.

The new tag appears in the list of device tags.

# Renaming a device tag

*To rename a device tag:*

1. In the main menu, go to **Repositories** → **Device tags**.
2. On the **Device tags** tab, select the tag that you want to rename.

   A tag properties window opens.
3. In the **Tag** field, change the tag name.
4. Click **Save** to save the changes.

The updated tag appears in the list of device tags.

# Deleting a device tag

You can delete only manually assigned tags.

*To delete a manually assigned device tag:*

1. In the main menu, go to **Repositories** → **Device tags**.

   The list of tags is displayed.
2. On the **Device tags** tab, select device tags that you want to delete.
3. Next, click the **Delete** button.
4. In the window that opens, click **Yes**.

The device tag is deleted. The deleted tag is automatically removed from all of the devices to which it was assigned.

When you delete a tag assigned to the device by an auto-tagging rule, the rule is not deleted, and the tag will be assigned to a new device when the device first meets the rule conditions. If you delete an auto-tagging rule, the tag specified in the rule conditions will be removed from all devices to which it was assigned but will not be deleted from the list of tags. If necessary, you can manually delete the tag from the list.

The deleted tag is not removed automatically from the device if this tag is assigned to the device by an application or Network Agent. To manage such tags, use the klscflag utility.

# Viewing devices to which a tag is assigned

*To view devices to which a tag is assigned:*

1. In the main menu, go to **Repositories** → **Device tags**.
2. On the **Device tags** tab, click the **View devices** link next to the tag for which you want to view the list of assigned devices.

   You will be redirected to the **Managed devices** section of the main menu, with the devices filtered by the tag for which you clicked the **View devices** link.
3. If you want to return to the list of device tags, click the **Back** button of your browser.

After you view the devices to which the tag is assigned, you can either create and assign a new tag or assign the existing tag to other devices. In this case, you have to remove the filter by tag, select the devices, and then assign the tag.

# Viewing tags assigned to a device

*To view tags assigned to a device:*

1. In the main menu, go to **Asset management** → **Managed devices**.
2. Click the name of the device whose tags you want to view.
3. In the device properties window that opens, select the **Tags** tab.

   The list of tags assigned to the selected device is displayed. In the **Tag assigned** column you can view how the tag was assigned.

In the toolbar, you can do the following:

- Assign another tag to the device.
- Remove an already assigned tag.
- View all device tags that exist on the Administration Server.

You cannot view the assigned tags locally on the device.

# Tagging a device manually

*To assign a tag to a device manually:*

1. View tags assigned to the device to which you want to assign another tag.
2. Click **Add**.
3. In the window that opens, do one of the following:
   - To create and assign a new tag, select **Create new tag**, and then specify the name of the new tag.
   - To select an existing tag, select **Assign existing tag**, and then select the necessary tag in the drop-down list.
4. Click **OK** to apply the changes.
5. Click **Save** to save changes.

The selected tag is assigned to the device.

# Removing an assigned tag from a device

*To remove a tag from a device:*

1. In the main menu, go to **Asset management** → **Managed devices**.
2. Click the name of the device whose tags you want to view.
3. In the device properties window that opens, select the **Tags** tab.
4. Select the check box next to the tag that you want to remove.
5. At the top of the list, click the **Unassign tag** button.
6. In the window that opens, click **OK**.

The tag is removed from the device.

The unassigned device tag is not deleted. If you want, you can delete it manually.

You cannot manually remove tags assigned to the device by applications or Network Agent. To manage these tags, use the klscflag utility.

# Viewing rules for tagging devices automatically

*To view rules for tagging devices automatically,*

Do one of the following:

- In the main menu, go to **Repositories** → **Device tags** → **Auto-tagging rules**.
- View tags assigned to a device and then click the **Set up auto-tagging rules** button.

The list of rules for auto-tagging devices appears.

# Editing a rule for tagging devices automatically

*To edit a rule for tagging devices automatically:*

1. View rules for tagging devices automatically.
2. Click the name of the rule that you want to edit.

   A rule settings window opens.
3. Edit the general properties of the rule:

   a. In the **Rule name** field, change the rule name.

   The name cannot contain more than 256 characters.

   b. Do one of the following:

   - Enable the rule by switching the toggle button to **Rule enabled**.
   - Disable the rule by switching the toggle button to **Rule disabled**.
4. Do one of the following:

   - If you want to add a new condition, click the **Add** button, and specify the settings of the new condition in the window that opens.
   - If you want to edit an existing condition, click the name of the condition that you want to edit, and then edit the condition settings.
   - If you want to delete a condition, select the check box next to the name of the condition that you want to delete, and then click **Delete**.
5. Click **OK** in the conditions settings window.
6. Click **Save** to save changes.

The edited rule is shown in the list.

# Creating a rule for tagging devices automatically

*To create a rule for tagging devices automatically:*

1. View rules for tagging devices automatically.
2. Click the **Add** button.

   A new rule settings window opens.
3. Configure the general properties of the rule:

   a. In the **Rule name** field, enter the rule name.

   The name cannot be more than 256 characters long.

   b. Do one of the following:

   - Enable the rule by switching the toggle button to **Rule enabled**.
   - Disable the rule by switching the toggle button to **Rule disabled**.

   c. In the **Tag** field, enter the new device tag name or select one of the existing device tags from the list.

   The name cannot be more than 256 characters long.
4. In the conditions section, click the **Add** button to add a new condition.

   A new condition settings window open.
5. Enter the condition name.

   The name cannot be more than 256 characters long. The name must be unique within a rule.
6. Configure the rule to trigger on the following conditions (you can select multiple conditions):

   - **Network**—Network properties of the device, such as DNS name of the device or device inclusion in an IP subnet.

     If case sensitive collation is set for the database that you use for Kaspersky Security Center Linux, keep case when you specify a device DNS name. Otherwise, the auto-tagging rule will not work.

   - **Applications**—Presence of Network Agent on the device, operating system type, version, architecture, and package manager.
   - **Virtual machines**—Device belongs to a specific type of virtual machine.
   - **Applications registry**—Presence of applications of different vendors on the device.

- **Custom parameters**—Presence of custom settings on the Android device or their compliance with the specified requirements. For detailed information on using custom settings, refer to the Kaspersky Secure Mobility Management Help.

  Custom settings are available only with the Kaspersky Mobile Devices Protection and Management plug-in 10.59.4.32 or later installed.

7. Click **OK** to save the changes.

   If necessary, you can set multiple conditions for a single rule. In this case, the tag will be assigned to a device if it meets at least one condition.

8. Click **Save** to save changes.

The newly created rule is enforced on devices managed by the selected Administration Server. If the settings of a device meet the rule conditions, the device is assigned the tag.

Later, the rule is applied in the following cases:

- Automatically and periodically, depending on the server workload
- After you edit the rule
- When you run the rule manually
- After Administration Server detects a change in the settings of a device that meets the rule conditions or the settings of a group that contains such a device

You can create multiple tagging rules. A single device can be assigned multiple tags if you have created multiple tagging rules and if the respective conditions of these rules are met simultaneously. You can view the list of all assigned tags in the device properties.

# Running rules for auto-tagging devices

When a rule is run, the tag specified in properties of this rule is assigned to devices that meet conditions specified in properties of the same rule. You can run only active rules.

*To run rules for auto-tagging devices:*

1. View rules for tagging devices automatically.
2. Select check boxes next to active rules that you want to run.
3. Click the **Run rule** button.

The selected rules are run.

# Deleting a rule for tagging devices automatically

*To delete a rule for tagging devices automatically:*

1. View rules for tagging devices automatically.
2. Select the check box next to the rule that you want to delete.
3. Click the **Delete** button.
4. In the window that opens, click **OK**.

The selected rule is deleted. The tag that was specified in properties of this rule is unassigned from all of the devices that it was assigned to.

The unassigned device tag is not deleted. If you want, you can delete it manually.

# Managing device tags by using the klscflag utility

To assign a set of tags to a device, you need to run the klscflag utility on the client device to which you want to assign tags.

The klscflag utility overwrites the existing tags assigned to the device. This means that you can add or remove tags by specifying the desired set of tags in the command. The utility does not have separate commands for adding or removing individual tags. Instead, you modify the entire set of tags.

When specifying tag names in commands like klscflag, it is recommended to use a consistent-case approach, such as all caps. Using all caps can help avoid potential issues with tags that differ only in case, depending on the DBMS configuration.

*To assign one or several tags to your device by using the klscflag utility:*

1. Run the command prompt under an account with root privileges, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where Network Agent is installed. The default installation directory is /opt/kaspersky/klnagent64/sbin/.
2. Enter one of the following commands:
   - To assign a set of tags:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"TAG NAME 1\",\"TAG NAME
     2\",\"TAG NAME 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     where `[\"TAG NAME 1\",\"TAG NAME 2\",\"TAG NAME 3\"]` is the list of tags that you want to assign to your device.

     If you leave the square brackets empty, this will remove all tags from the device:

```
/opt/kaspersky/klnagent64/sbin/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\";"
```

- To assign a new tag to an existing set of tags:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
  KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NEW TAG NAME\",\"TAG NAME
  1\",\"TAG NAME 2\",\"TAG NAME 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

  where `NEW TAG NAME` is the name of the tag that you want to assign to your device and `TAG NAME 1`, `TAG NAME 2`, `TAG NAME 3` are the names of the tags already assigned to the device.

- To remove a specific tag without removing other tags already assigned to the device, run the command with the updated set of tags.

  For example, if your current tags are `TAG NAME 1`, `TAG NAME 2`, `TAG NAME 3` and you want to remove `TAG NAME 2`, run the following command:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
  KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"TAG NAME 1\",\"TAG NAME 3\"]" -
  svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

3. Run the following command to restart the Network Agent service:

   ```
   systemctl restart klnagent
   ```

   The klscflag utility assigns the specified tags to your device.

4. If you want to make sure that the klscflag utility has assigned the specified tags successfully, view tags assigned to the device.

Alternatively, you can assign device tags manually.

# Data encryption and protection

Data encryption reduces the risk of unintentional leakage of sensitive and corporate data if your laptop or hard drive is stolen or lost. Also, data encryption allows you to prevent access by unauthorized users and applications.

You can use the data encryption feature if your network includes Windows-based managed devices with Kaspersky Endpoint Security for Windows installed. In this case, on devices running a Windows operating system, you can manage the following types of encryption:

- BitLocker Drive Encryption
- Kaspersky Disk Encryption

> We do not recommend enabling encryption in VDI.

By using these components of Kaspersky Endpoint Security for Windows, you can, for example, enable or disable encryption, view the list of encrypted drives, or generate and view reports about encryption.

To configure encryption, define the Kaspersky Endpoint Security for Windows policy in Kaspersky Security Center Linux. Kaspersky Endpoint Security for Windows performs encryption and decryption according to the active policy. For detailed instructions on how to configure rules and for a description of encryption features, see the Kaspersky Endpoint Security for Windows Help.

Encryption management for a hierarchy of Administration Servers is currently not available in the Web Console. Use the primary Administration Server to manage encrypted devices.

You can show or hide some of the interface elements related to the encryption management feature by using the user interface settings.

# Viewing the list of encrypted drives

In Kaspersky Security Center Linux, you can view details about encrypted drives and devices that are encrypted at the drive level. After the information on a drive is decrypted, the drive is automatically removed from the list.

*To view the list of encrypted drives,*

In the main menu, go to **Operations** → **Data encryption and protection** → **Encrypted drives**.

If the section is not on the menu, this means that it is hidden. In the user interface settings, enable the **Show data encryption and protection** option to display the section.

You can export the list of encrypted drives to a CSV or TXT file. To do this, click the **Export to CSV** or **Export to TXT** button.

# Viewing the list of encryption events

When running data encryption or decryption tasks on devices, Kaspersky Endpoint Security for Windows sends Kaspersky Security Center Linux information about events of the following types:

- Cannot encrypt or decrypt a file, or create an encrypted archive, due to a lack of free disk space.
- Cannot encrypt or decrypt a file, or create an encrypted archive, due to license issues.
- Cannot encrypt or decrypt a file, or create an encrypted archive, due to missing access rights.
- The application has been prohibited from accessing an encrypted file.
- Unknown errors.

*To view a list of events that occurred during data encryption on devices,*

In the main menu, go to **Operations** → **Data encryption and protection** → **Encryption events**.

If the section is not on the menu, this means that it is hidden. In the user interface settings, enable the **Show data encryption and protection** option to display the section.

You can export the list of encrypted drives to a CSV or TXT file. To do this, click the **Export to CSV** or **Export to TXT** button.

Alternatively, you can examine the list of encryption events for every managed device.

*To view the encryption events for a managed device:*

1. In the main menu, go to the **Asset management** → **Managed devices** section.
2. Click on the name of a managed device.
3. On the **General** tab, go to the **Protection** section.
4. Click the **View data encryption errors** link.

# Creating and viewing encryption reports

You can generate the following reports:

- Report on encryption status of managed devices. This report provides details about the data encryption of various managed devices. For example, the report shows the number of devices to which the policy with configured encryption rules applies. Also, you can find out, for instance, how many devices need to be rebooted. The report also contains information about the encryption technology and algorithm for every device.
- Report on encryption status of mass storage devices. This report contains similar information as the report on the encryption status of managed devices, but it provides data only for mass storage devices and removable drives.
- Report on rights to access encrypted drives. This report shows which user accounts have access to encrypted drives.
- Report on file encryption errors. This report contains information about errors that occurred when the data encryption or decryption tasks were run on devices.
- Report on blockage of access to encrypted files. This report contains information about blocking application access to encrypted files. This report is helpful if an unauthorized user or application tries to access encrypted files or drives.

You can generate any report in the **Monitoring** → **Reports** section. Alternatively, in the **Operations** → **Data encryption and protection** section, you can generate the following encryption reports:

- Report on encryption status of mass storage devices
- Report on rights to access encrypted drives
- Report on file encryption errors

*To generate an encryption report in the **Data encryption and protection** section:*

1. Make sure that you enabled the **Show data encryption and protection** option in the Interface options.
2. In the main menu, go to **Operations** → **Data encryption and protection**.

3. Open one of the following sections:

   - **Encrypted drives** generates the report on encryption status of mass storage devices or the report on rights to access encrypted drives.
   - **Encryption events** generates the report on file encryption errors.

4. Click the name of the report that you want to generate.

The report generation starts.

# Granting access to an encrypted drive in offline mode

A user can request access to an encrypted device, for example, when Kaspersky Endpoint Security is not installed on the managed device. After you receive the request, you can create an access key file and send it to the user. All of the use cases and detailed instructions are provided in the Kaspersky Endpoint Security Help for the required platform.

*To grant access to an encrypted drive in offline mode in Kaspersky Endpoint Security for Windows:*

1. Get a request access file from a user (a file with the FDERTC extension). Follow the instructions in the Kaspersky Endpoint Security for Windows Help to generate the file in Kaspersky Endpoint Security for Windows.
2. In the main menu, go to **Operations** → **Data encryption and protection** → **Encrypted drives**.

   A list of encrypted drives appears.
3. Select the drive to which the user requested access.
4. Click the **Grant access to the device in offline mode** button.
5. In the window that opens, select the Kaspersky Endpoint Security for Windows plug-in.
6. Follow the instructions provided in the Kaspersky Endpoint Security for Windows Help (see the instructions for Kaspersky Security Center Web Console at the end of the section).

After that, the user applies the received file to access the encrypted drive and read data stored on the drive.

# Transmitting encryption keys between Administration Servers

If the data encryption feature is enabled on a managed device, the encryption key is stored on the Administration Server. The encryption key is used to access encrypted data and to manage the encryption policy.

The encryption key must be transmitted to another Administration Server in the following cases:

- Reconfiguring Network Agent on a managed device to assign the device to another Administration Server. If this device contains encrypted data, the encryption key must be transmitted to the target Administration Server. Otherwise, the data cannot be decrypted.

- Encrypting a removable drive connected to a device D1 that is managed by the Administration Server S1, and then you connect this removable drive to a device D2 managed by the Administration Server S2. To access to the data on the removable drive, the encryption key must be transmitted from the Administration Server S1 to the Administration Server S2.

- Encrypting a file on a device D1 managed by the Administration Server S1, and then you try to access the file on a device D2 managed by the Administration Server S2. To access the file, the encryption key must be transmitted from the Administration Server S1 to the Administration Server S2.

You can transmit encryption keys the following ways:

- Automatically, by enabling the **Use hierarchy of Administration Servers to obtain encryption keys** option in the properties of two Administration Servers between which an encryption key must be transmitted. If this option is disabled for one of the Administration Servers, the automatic transmission of encryption keys is not possible.

  When you enable the **Use hierarchy of Administration Servers to obtain encryption keys** option in an Administration Server properties, the Administration Server sends all of the encryption keys stored in its repository to the primary Administration Server (if any) one level up in the hierarchy.

  When you try to access encrypted data, the Administration Server first searches the encryption key in its own repository. If the **Use hierarchy of Administration Servers to obtain encryption keys** option is enabled and the required encryption key has not been found in the repository, the Administration Server additionally sends a request to the primary Administration Servers (if any) to provide the required encryption key. The request will be sent to all of the primary Administration Servers up to the server on the highest level of the hierarchy.

- Manually from one Administration Server to another by exporting and importing the file containing the encryption keys.

  The export and import of encryption keys are actions that are included in the Encryption key management feature. To perform these actions, configure the access rights to the feature for users of Kaspersky Security Center Linux as follows:

  - Grant the **Read** access right to the Encryption key management feature for a user that exports encryption keys from the secondary Administration Server.

  - Grant the **Write** access right to the Encryption key management feature for a user that imports encryption keys to the target Administration Server.

*To enable automatic transmission of encryption keys between Administration Servers within the hierarchy:*

1. Go to the properties of the required Administration Server:

   a. In the main menu, select a section (except for **Marketplace**, **Console navigation**, and **Settings**), and then at the top of the page, click the **Show hierarchy** button.

   b. In the navigation pane that opens, hover the mouse cursor over the name of the required Administration Server, and then click the settings icon (⚙).

   Alternately, you can click the Administration Server name, and then, after the name is displayed in the main menu, click it in the main menu to open the server properties window.

2. In the properties window that opens, select the **Encryption algorithm** section.

3. Enable the **Use hierarchy of Administration Servers to obtain encryption keys** option.

4. Click **Save** to apply changes.

The encryption keys will be transmitted to primary Administration Servers (if any) at the next synchronization (the heartbeat). This Administration Server will also provide, upon request, an encryption key from its repository to a secondary Administration Server.

*To transmit encryption keys between Administration Servers manually:*

1. Go to the properties of the Administration Server from which you want to export encryption keys:

   a. In the main menu, select a section (except for **Marketplace**, **Console navigation**, and **Settings**), and then at the top of the page, click the **Show hierarchy** button.

   b. In the navigation pane that opens, hover the mouse cursor over the name of the required Administration Server, and then click the settings icon (⚙).

   Alternately, you can click the Administration Server name, and then, after the name is displayed in the main menu, click it in the main menu to open the server properties window.

2. In the properties window that opens, select the **Encryption algorithm** section.

3. Click **Export encryption keys**.

   Make sure that a user that exports encryption keys from the Server is granted the **Read** access right to the Encryption key management feature.

4. In the **Export encryption keys from Administration Server?** window do the following:

   a. Specify a password to protect the file from unauthorized access.

   b. Specify where you want to save the file.

   Remember the password. A lost password cannot be retrieved. If the password is lost, you have to repeat the export procedure. Therefore, make a note of the password and keep it handy.

5. Transmit the file to another Administration Server, for example, through a shared folder or removable drive.

6. Go to the properties of the Administration Server to which you want to import the encryption keys.

7. In the properties window, select the **Encryption algorithm** section.

8. Click **Import encryption keys**.

   Make sure that a user that imports encryption keys to the Server is granted the **Write** access right to the Encryption key management feature.

9. Select the file containing the encryption keys.

10. Enter the password and click **OK**.

The encryption keys are transmitted to the target Administration Server.

# Changing the Administration Server for client devices

You can change the Administration Server to a different one for specific client devices. For this purpose, use the *Change Administration Server* task.

*To change the Administration Server that manages client devices to a different Server:*

1. Connect to the Administration Server that manages the devices.
2. Create the Administration Server change task.

   The New task wizard starts. Follow the steps of the wizard. In the **New task** window of the New task wizard, select the **Kaspersky Security Center 17** application and the **Change Administration Server** task type. After that, specify the devices for which you want to change the Administration Server:

   - **Assign task to an administration group**

     The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

     For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

     If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

   - **Specify device addresses manually or import addresses from a list**

     You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

     You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

   - **Assign task to a device selection**

     The task is assigned to devices included in a device selection. You can specify one of the existing selections.

     For example, you may want to use this option to run a task on devices with a specific operating system version.

3. Run the created task.

After the task is completed, the client devices for which it was created are put under the management of the Administration Server specified in the task settings.

If the Administration Server supports encryption and data protection and you are creating a *Change Administration Server* task, a warning is displayed. The warning states that if any encrypted data is stored on devices, after the new Server begins managing the devices, users will be able to access only the encrypted data with which they previously worked. In other cases, no access to encrypted data is provided. For detailed descriptions of scenarios in which access to encrypted data is not provided, refer to the Kaspersky Endpoint Security for Windows Help.

# Avoiding conflicts between multiple Administration Servers

If you have more than one Administration Server on your network, they can see the same client devices. This may result, for example, of Administration Server installing an application that was already installed by another Administration Server, and other conflicts. To prevent an application from being installed on a device managed by another Administration Server, you must enable the **Install only on devices managed through this Administration Server** option in the *Install application remotely* task properties.

If you enable the **Install only on devices managed through this Administration Server** option, and then run the *Install application remotely* task, a check is performed to determine if the devices are managed by another Administration Server. For devices managed by another Administration Server, the **Managed by a different Administration Server** attribute value will be set to `true`. The *Install application remotely* task will not be applied to these devices.

The **Managed by a different Administration Server** attribute values are displayed in the **Managed by a different Administration Server** column in the list of managed devices and list of unassigned devices.

You can also use the **Managed by a different Administration Server** property as a criterion for the following purposes:

- Displaying managed devices
- Device selections
- Device moving rules
- Auto-tagging rules

*To reset the Managed by a different Administration Server attribute:*

1. In the main menu of Kaspersky Security Center Web Console, go to **Asset management** → **Unassigned devices**.
2. Select the required device, and then click the **Remove the Managed by a different Administration Server attribute** button.

The **Managed by a different Administration Server** attribute is reset.

# Moving devices connected to Administration Server through connection gateways to another Administration Server

You can move devices connected to the Administration Server through connection gateways to another Administration Server. For example, this may be required if you install another version of Administration Server and do not want to reinstall Network Agent on the devices as it may be time consuming.

> The commands described in the instruction must be run on client devices under an account with administrator rights.

*To move a device connected through the connection gateway to another Administration Server:*

1. Run the klmover utility with the `-address <server address>` parameter, to switch to the new Administration Server.
2. Run the `klnagchk -nagwait -tl 4` command.
3. Run the following commands to set a new connection gateway:
   - `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\";"`

     Here `<gateway ip or name>` is the address of the connection gateway accessible from the internet.
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     The `13000` is the number of the TCP port that the connection gateway is listening to.
4. Run the `klnagchk -restart -tl 4` command to start the Network Agent service.

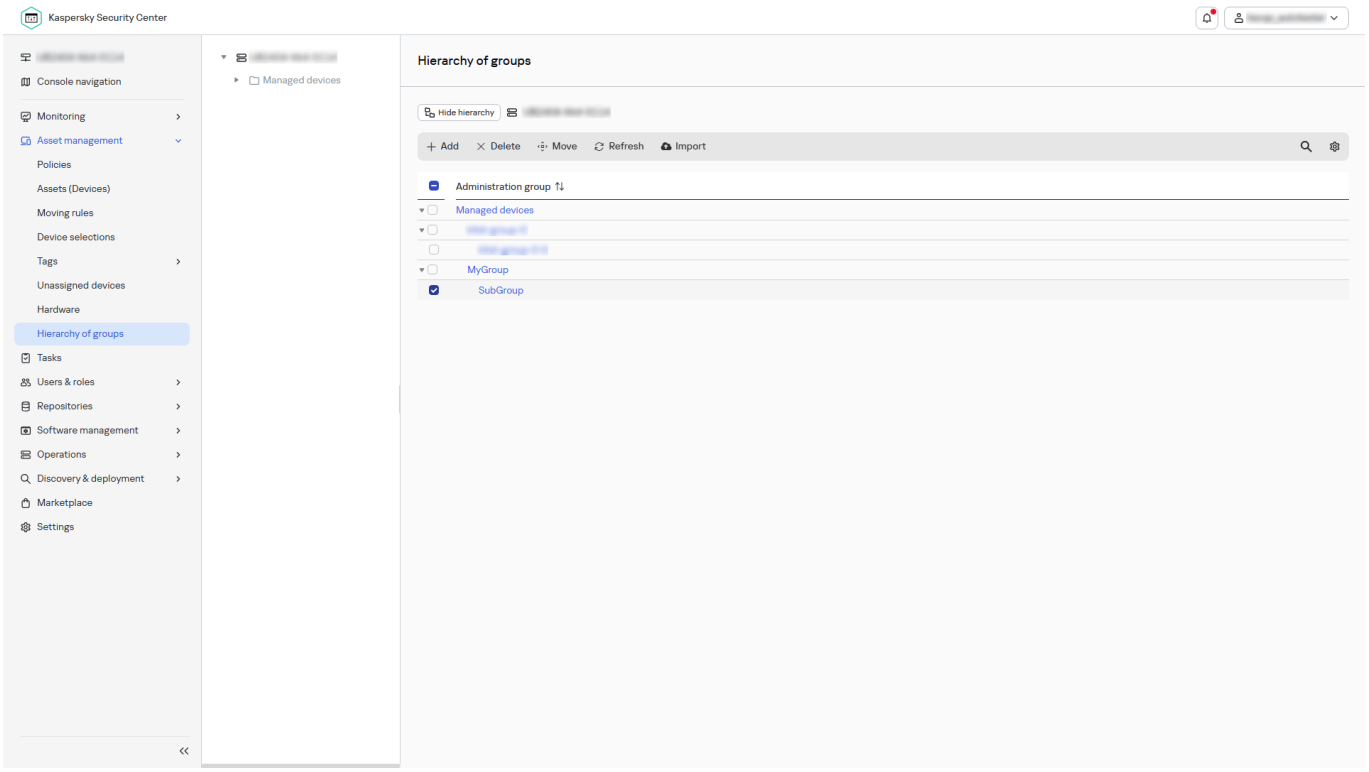
The device is moved to the new Administration Server and connected through the new connected gateway.

# Viewing and configuring the actions when devices show inactivity

If client devices within a group are inactive, you can get notifications about it. You can also automatically delete such devices.

*To view or configure the actions when the devices in the group show inactivity:*

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. Go to the properties of the required administration group in one of the following ways:
   - Click the name of the administration group.
   - Click the **Show hierarchy** button at the top of the page. In the navigation pane that opens, hover the mouse cursor over the name of the required group, and then click the settings icon ( ⚙ ).




Administration group hierarchy

   The administration group properties window opens.

3. In the properties window, go to the **Settings** tab.
4. In the **Inheritance** section, enable or disable the following options:

   **Inherit from parent group**

   The settings in this section will be inherited from the parent group in which the client device is included. If this option is enabled, the settings under **Device activity on the network** are locked from any changes.

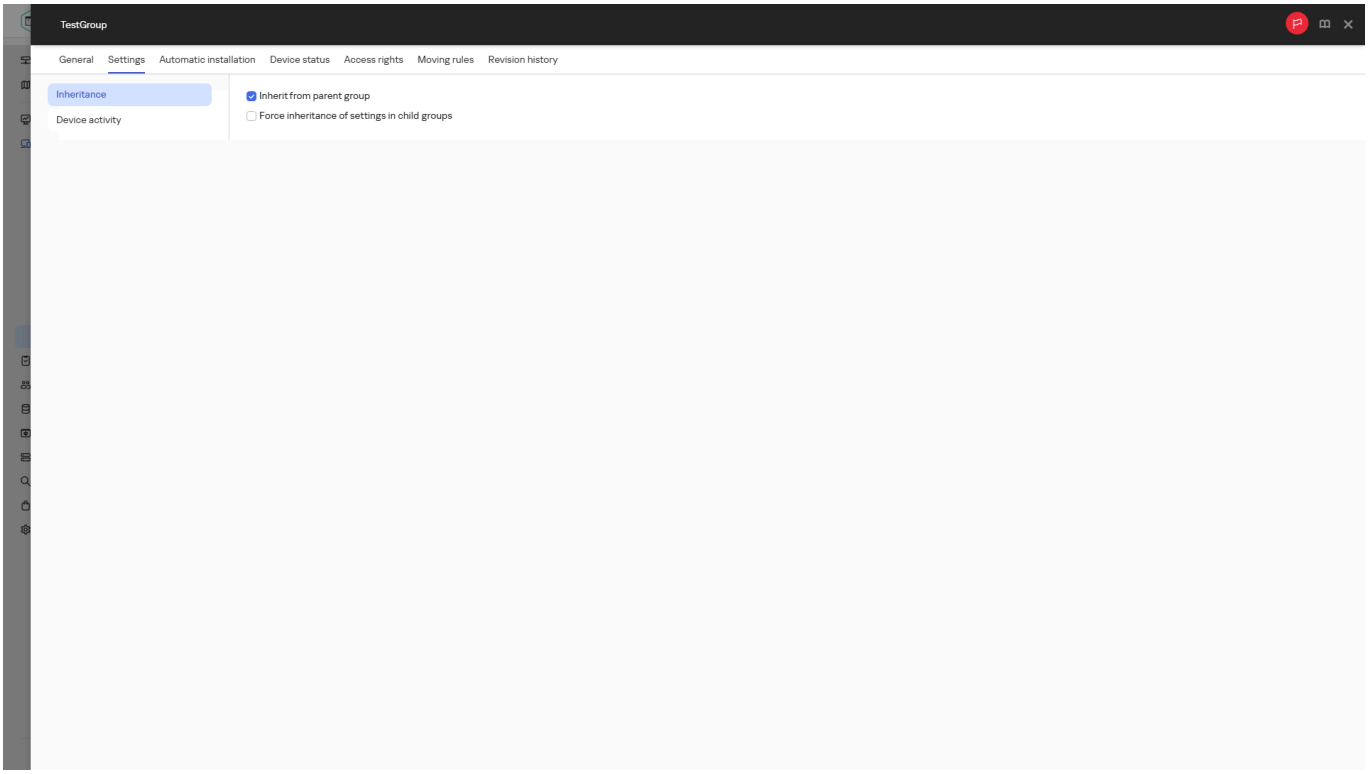
   This option is available only if the administration group has a parent group.

   By default, the option is enabled.

   **Force inheritance of settings in child groups**

   The setting values will be distributed to child groups but in the properties of the child groups these settings are locked.

By default, this option is disabled.




Administration group properties

5. In the **Device activity** section, enable or disable the following options:

   **Notify the administrator if the device has been inactive for longer than (days)**

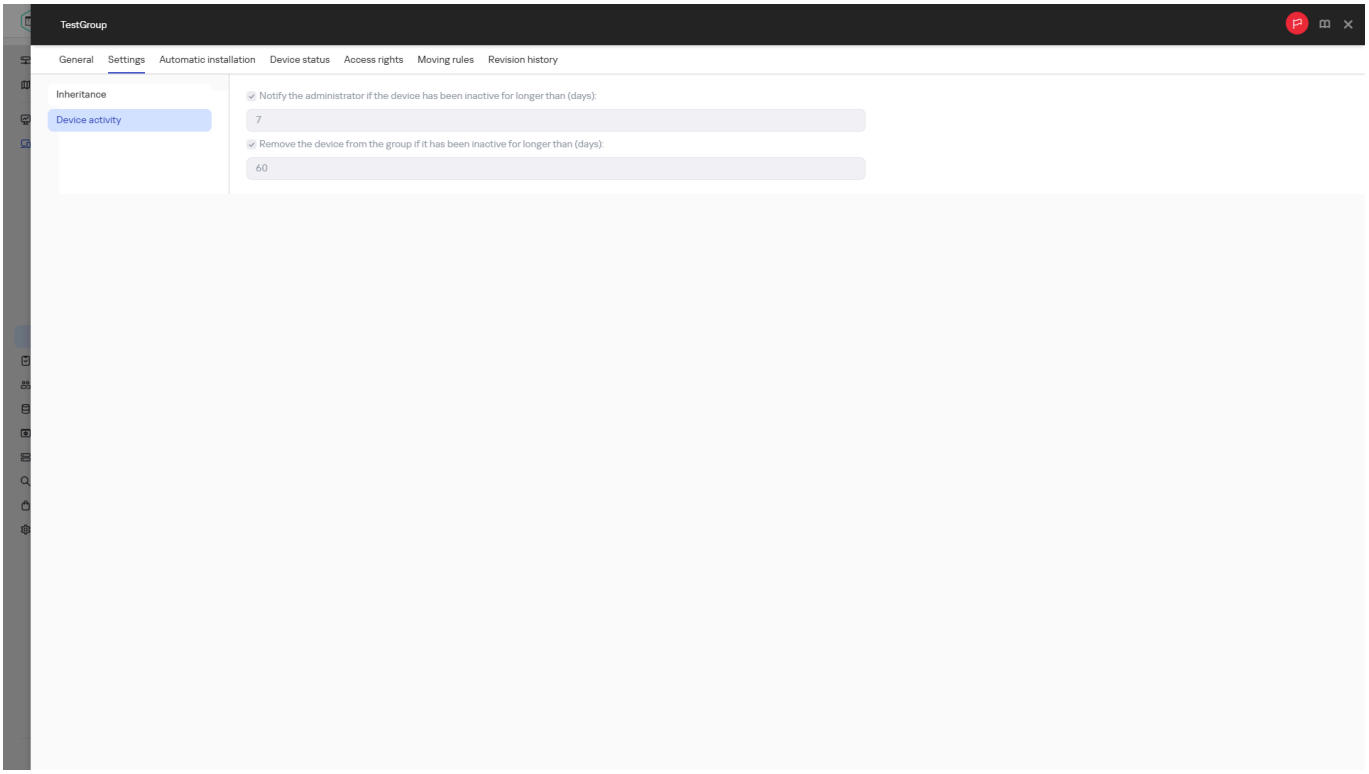
   If this option is enabled, the administrator receives notifications about inactive devices. You can specify the time interval after which the **Device has remained inactive on the network in a long time** event is created. The default time interval is 7 days.

   By default, the option is enabled.

   **Remove the device from the group if it has been inactive for longer than (days)**

   If this option is enabled, you can specify the time interval after which the device is automatically removed from the group. The default time interval is 60 days.

By default, the option is enabled.




Administration group properties

6. Click the **Save** button.

Your changes are saved and applied.

# Sending messages to device users

*To send a message to users of devices:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts.
3. In the **Task type** drop-down list, select **Send message to user**.
4. Select an option to specify the administration group, the device selection, or the devices to which the task applies.
5. Run the created task.

After the task is completed, the created message will be sent to the users of the selected devices. The **Send message to user** task is available only for devices running Windows.

# Turning on, turning off, and restarting client devices remotely

Kaspersky Security Center Linux allows you to manage client devices remotely by turning on, shutting down, or restarting them.

*To remotely manage client devices:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts.
3. In the **Task type** drop-down list, select **Manage devices**.
4. Select an option to specify the administration group, the device selection, or the devices to which the task applies.
5. Select the command (turn on, turn off, or restart).
6. If necessary, configure the following settings for the turn off and restart commands:

   - Turn on the **Prompt user for confirmation** toggle button to specify the user prompt message and the time intervals after which you want to repeat the prompt and to restart or turn of the devices.
   - Select the **Wait time before forced closure of applications in blocked sessions (min)** check box and specify the time.

   These settings are applicable to Windows client devices only. Linux devices will be restarted or turned off immediately after the task is complete.
7. Run the created task.

After the task is completed, the command (turn on, turn off, or restart) will be executed on the selected devices.

# Remote access to managed devices

Kaspersky Security Center Linux allows you to establish a remote connection to managed devices. The administrator can obtain remote access to the managed device through a Network Agent installed on the device. Remote connection to a device through the Network Agent is possible even if the TCP and UDP ports of the client device are closed. Upon establishing a connection with the device, the administrator gains full access to information stored on this device and can manage applications installed on it.

The methods for establishing a remote connection depend on which platform is used on the device with Kaspersky Security Center Web Console. Kaspersky Security Center Web Console can be installed on a device other than the Administration Server device, on a Windows- or a Linux-based device.

From Kaspersky Security Center Web Console installed on a Linux device, you can establish the following connections:

- To a Linux-based managed device by using:
  - Remote desktop connection (RDP)
  - Virtual Network Computing (VNC)
- To a Windows-based managed device by using:
  - Remote desktop connection (RDP)
  - Virtual Network Computing (VNC)

From Kaspersky Security Center Web Console installed on a Windows device, you can establish the following connections:

- To a Linux-based managed device by using:
  - Remote desktop connection (RDP)
  - Virtual Network Computing (VNC)
- To a Windows-based managed device by using:
  - Remote desktop connection (RDP)
  - Windows Desktop Sharing (WDS)

Remote connection to managed devices is not supported when accessing the Kaspersky Security Center Web Console from a device running Microsoft Windows on Arm.

To establish a remote connection to a device, you must have the following:

- klsctunnel utility

  The Kaspersky utility is used for tunneling the connection between a managed device and Administration Server.

  Kaspersky Security Center Linux allows tunneling TCP connections from Kaspersky Security Center Web Console via the Administration Server and then via Network Agent to a specified port on a managed device. Tunneling is designed for connecting a client application on a device with Kaspersky Security Center Web Console installed to a TCP port on a managed device—if no direct connection is possible between Kaspersky Security Center Web Console and the target device.

  Connection tunneling between a remote client device and Administration Server is required if the port used for connection to Administration Server is not available on the device. The port on the device may be unavailable in the following cases:

  - The remote device is connected to a local network that uses the NAT mechanism.
  - The remote device is part of the local network of Administration Server, but its port is closed by a firewall.

  You can download the utility from Kaspersky Security Center Web Console if a remote connection is established using the Web Console, or manually from the Kaspersky website.

The klsctunnel utility is installed on the Administration Server device and used for all types of the remote connection (RDP, VNC, WDS).

- RDP or VNC client

  An RDP or VNC client is installed on the Administration Server device. This client allows you to obtain remote access to the managed device by using the address and port for the local connection provided by the klsctunnel utility.

  An RDP connection to the current remote desktop session of the user is established without the user's knowledge. Once the administrator connects to the session, the device user is disconnected from the session without notification.

- Windows Desktop Sharing (only for Windows-based managed devices)

  This feature allows you to connect to an existing session on a client device without disconnecting the user in this session. In this case, the administrator and the session user on the device share access to the desktop.

  When connecting to an existing session of the remote desktop, the session user on the device receives a connection request from the administrator. No information about remote activity on the device and its results will be saved in reports created by Kaspersky Security Center Linux.

  The administrator can configure an audit of user activity on a remote client device. During the audit, the application saves information about files on the client device that have been opened and/or modified by the administrator.

# Remote access from a Linux-based device with Kaspersky Security Center Web Console to a Linux-based managed device

Prerequisites

Before you start, make sure that you have done the following:

- On the managed device running Linux, Network Agent version 15.3 or later is installed.
- On the managed device running Linux, the RDP server is installed (if you connect to the managed device by using Remote Desktop Connection).
- On the managed device running Linux, the VNC server is installed (if you connect to the managed device by using Virtual Network Computing).
- Port for tunneling RDP connections is opened (the **Open port for tunneling RDP connections** option is enabled in the **Connection ports** section of the Administration Server properties window).
- The administrator has the **Start RDP sessions** right to establish RDP connections (if you connect to the managed device by using Remote Desktop Connection).
- The administrator has the **Initiate tunneling** right to establish the tunnel connection for VNC (if you connect to the managed device by using Virtual Network Computing).

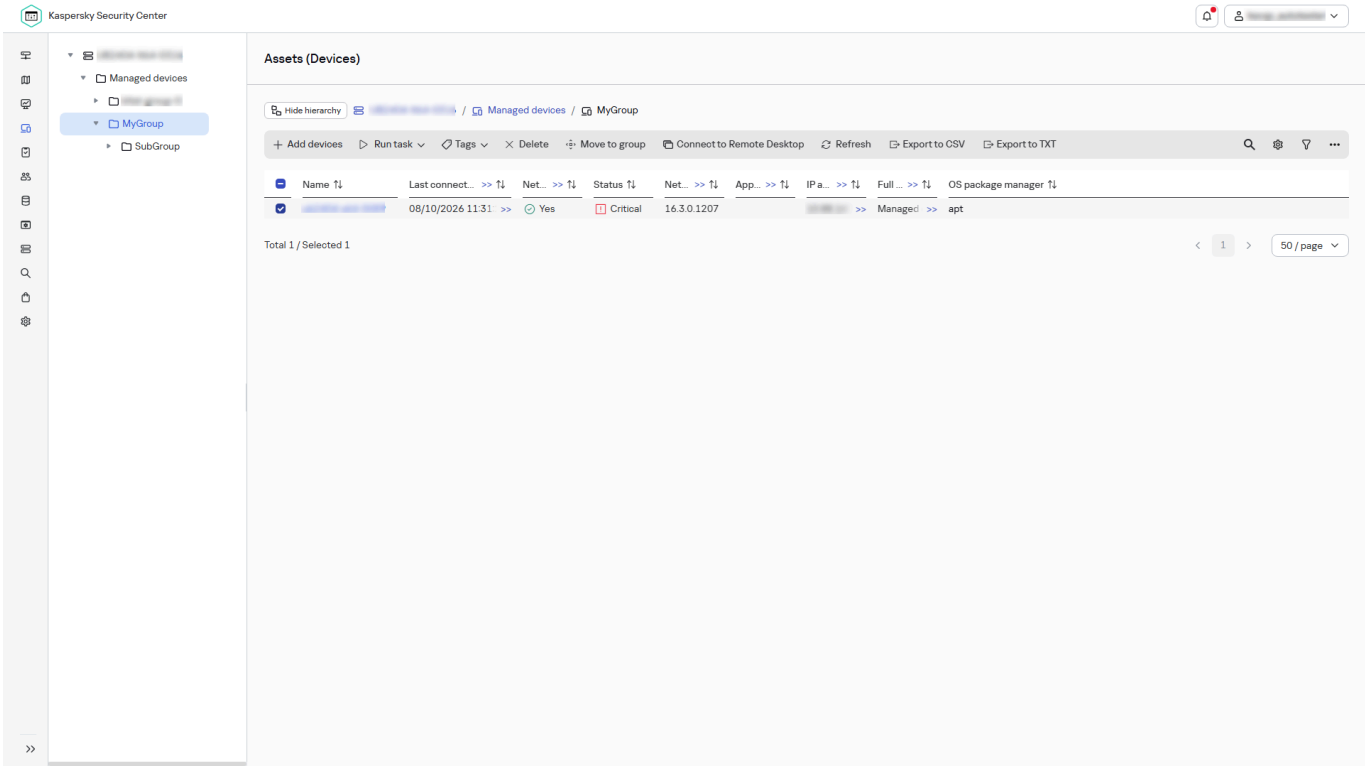
*To connect to a Linux-based managed device by using RDP or VNC through Kaspersky Security Center Web Console opened on a Linux-based device:*

1. In the main menu, go to the **Asset management** → **Managed devices** section or open a device selection.

2. Select the check box next to the managed device to which you want to connect remotely, and then click the **Connect to Remote Desktop** button.

   The **Connect to Remote Desktop** window opens.

   If you select multiple devices, a mobile device, or a device running macOS, the **Connect to Remote Desktop** button will be disabled.




The list of managed devices

3. Download the klsctunnel utility by clicking the **Download** button, and then run it.

   When downloading the utility, take into account the following:

   - To get an up-to-date version of the klsctunnel utility, make sure that Administration Server has access to Kaspersky update servers.

     You can run the *Download updates to the Administration Server repository* task and select Kaspersky update servers as a source of updates. If the task finishes successfully, Administration Server has access to Kaspersky update servers.

   - If the utility file is unavailable for download, an error message is displayed. In this case, download the utility manually, and then place it on the Administration Server device in the /var/opt/kaspersky/klnagent_srv directory.

4. In the **Connect to Remote Desktop** window, specify the connection port. The default port number is 3389.

5. Generate a text blob with encoded connection parameters by clicking the **Generate blob** button, and then copy and paste the text into the corresponding field in the klsctunnel utility.

   A blob contains the settings required to establish a connection between Administration Server and the managed device. A blob is valid for three minutes. If it has expired, generate a new blob.

6. In the klsctunnel utility, if you use a proxy server, specify the proxy server connection settings.

The klsctunnel utility displays the address and port for the local connection of a remote access client.

The utility allows the administrator to close the tunnel connection. If the tunnel connection is closed, the current connection to the remote desktop is terminated.

7. Run a remote access client (RDP or VNC) and connect it to the managed device by using the address and port provided by the klsctunnel utility.

The connection with the managed device is established. The desktop is available in the remote access client window.

# Remote access from a Linux-based device with Kaspersky Security Center Web Console to a Windows-based managed device

Remote desktop connection (RDP)

**Prerequisites**

Before you start, make sure that you have done the following:

- A remote connection is allowed in the operating system settings of the managed device.
- On the managed device running Windows, Network Agent version 13 or later is installed.
- The administrator has the **Start RDP sessions** right to establish RDP connections.
- Port for tunneling RDP connections is opened (the **Open port for tunneling RDP connections** option is enabled in the **Connection ports** section of the Administration Server properties window).

*To connect to a Windows-based managed device by using RDP through Kaspersky Security Center Web Console opened on a Linux-based device:*

1. In the main menu, go to the **Asset management** → **Managed devices** section or open a device selection.
2. Select the check box next to the managed device to which you want to connect remotely, and then click the **Connect to Remote Desktop** button.

   The **Connect to Remote Desktop** window opens.

   If you select multiple devices, a mobile device, or a device running macOS, the **Connect to Remote Desktop** button will be disabled.
3. In the **Connect to Remote Desktop** window, select the **RDP** connection type.
4. If a remote connection is not allowed in the operating system settings of the managed device, allow the remote connection centrally by clicking the **Change settings** button.

   If the settings are applied correctly, a notification is displayed. Also, on the managed device, in the **Settings** → **System** → **Remote Desktop** section, the **Enable Remote Desktop** option is enabled.

   If the remote connection is allowed in the operating system settings of the managed device, the **Change settings** button is not displayed.

5. Download the klsctunnel utility by clicking the **Download** button, and then run it.

   When downloading the utility, take into account the following:

   - To get an up-to-date version of the klsctunnel utility, make sure that Administration Server has access to Kaspersky update servers.

     You can run the *Download updates to the Administration Server repository* task and select Kaspersky update servers as a source of updates. If the task finishes successfully, Administration Server has access to Kaspersky update servers.

   - If the utility file is unavailable for download, an error message is displayed. In this case, download the utility manually, and then place it on the Administration Server device in the /var/opt/kaspersky/klnagent_srv directory.

6. Generate a text blob with encoded connection parameters by clicking the **Generate blob** button, and then copy and paste the text into the corresponding field in the klsctunnel utility.

   A blob contains the settings required to establish a connection between Administration Server and the managed device. A blob is valid for three minutes. If it has expired, generate a new blob.

7. In the klsctunnel utility, if you use a proxy server, specify the proxy server connection settings.

   The klsctunnel utility displays the address and port of the connection to the remote device.

   The utility allows the administrator to close the tunnel connection. If the tunnel connection is closed, the current connection to the remote desktop is terminated.

8. Run an RDP client and connect it to the managed device by using the address and port provided by the klsctunnel utility.

The connection with the managed device is established. The desktop is available in the RDP client window.

Connection to the current remote desktop session of the user is established without the user's knowledge. Once the administrator connects to the session, the device user is disconnected from the session without notification.

Virtual Network Computing system (VNC)

**Prerequisites**

Before you start, make sure that you have done the following:

- On the managed device running Windows, Network Agent version 13 or later is installed.
- On the managed device running Windows, the VNC server is installed.
- The administrator has the **Initiate tunneling** right to establish the tunnel connection for VNC.
- Port for tunneling RDP connections is opened (the **Open port for tunneling RDP connections** option is enabled in the **Connection ports** section of the Administration Server properties window).

*To connect to a Windows-based managed device by using VNC through Kaspersky Security Center Web Console opened on a Linux-based device:*

1. In the main menu, go to the **Asset management** → **Managed devices** section or open a device selection.
2. Select the check box next to the managed device to which you want to connect remotely, and then click the **Connect to Remote Desktop** button.

   The **Connect to Remote Desktop** window opens.

   If you select multiple devices, a mobile device, or a device running macOS, the **Connect to Remote Desktop** button will be disabled.
3. In the **Connect to Remote Desktop** window, select the connection type **VNC**.
4. Download the klsctunnel utility by clicking the **Download** button, and then run it.

   If the utility file is unavailable for download, an error message is displayed. In this case, download the utility manually.
5. In the **Connect to Remote Desktop** window, specify the VNC connection port. The default port number is 5900.
6. Generate a text blob with encoded connection parameters by clicking the **Generate blob** button, and then copy and paste the text into the corresponding field in the klsctunnel utility.

   A blob contains the settings required to establish a connection between Administration Server and the managed device. A blob is valid for three minutes. If it has expired, generate a new blob.
7. In the klsctunnel utility, if you use a proxy server, specify the proxy server connection settings.

   The klsctunnel utility displays the address and port for the local connection of the VNC client.

   The utility allows the remote user to close the tunnel connection. If the tunnel connection is closed, the current connection to the remote desktop is terminated.
8. Run a VNC client and connect it to the managed device by using the address and port provided by the klsctunnel utility.

The connection with the managed device is established. The desktop is available in the VNC client window.

# Remote access from a Windows-based device with Kaspersky Security Center Web Console to a Linux-based managed device

Remote desktop connection (RDP)

**Prerequisites**

Before you start, make sure that you have done the following:

- On the managed device running Linux, the RDP server is installed.
- On the managed device running Linux, Network Agent version 15.3 or later is installed.

- The administrator has the **Start RDP sessions** right to establish RDP connections.
- Port for tunneling RDP connections is opened (the **Open port for tunneling RDP connections** option is enabled in the **Connection ports** section of the Administration Server properties window).

*To connect to a Linux-based managed device by using RDP through Kaspersky Security Center Web Console opened on a Windows-based device:*

1. In the main menu, go to the **Asset management** → **Managed devices** section or open a device selection.
2. Select the check box next to the managed device to which you want to connect remotely, and then click the **Connect to Remote Desktop** button.

   The **Connect to Remote Desktop** window opens.

   If you select multiple devices, a mobile device, or a device running macOS, the **Connect to Remote Desktop** button will be disabled.
3. In the **Connect to Remote Desktop** window, select the **RDP** connection type.
4. Download the klsctunnel utility by clicking the **Download** button, and then run it.

   When downloading the utility, take into account the following:

   - To get an up-to-date version of the klsctunnel utility, make sure that Administration Server has access to Kaspersky update servers.

     You can run the *Download updates to the Administration Server repository* task and select Kaspersky update servers as a source of updates. If the task finishes successfully, Administration Server has access to Kaspersky update servers.
   - If the utility file is unavailable for download, an error message is displayed. In this case, download the utility manually, and then place it on the Administration Server device in the /var/opt/kaspersky/klnagent_srv directory.
5. Generate a text blob with encoded connection parameters by clicking the **Generate blob** button, and then copy and paste the text into the corresponding field in the klsctunnel utility.

   A blob contains the settings required to establish a connection between Administration Server and the managed device. A blob is valid for three minutes. If it has expired, generate a new blob.
6. In the klsctunnel utility, if you use a proxy server, specify the proxy server connection settings.

   To do this, select the **Use proxy server** check box, and then specify the connection settings.
7. Click the **Open port** button.

   The Remote Desktop Connection login window opens.
8. Specify the credentials of the account under which you are currently logged in to Kaspersky Security Center Web Console, and then connect to the managed device.

   The klsctunnel utility displays the address and port of the connection to the remote device.

   The utility allows the administrator to close the tunnel connection. If the tunnel connection is closed, the current connection to the remote desktop is terminated.

When connection to the device is established, the desktop is available in the Remote Desktop Connection window of Microsoft Windows.

Connection to the current remote desktop session of the user is established without the user's knowledge. Once the administrator connects to the session, the device user is disconnected from the session without notification.

Virtual Network Computing system (VNC)

**Prerequisites**

Before you start, make sure that you have done the following:

- On the managed device running Linux, Network Agent version 15.3 or later is installed.
- On the managed device running Linux, the VNC server is installed.
- The administrator has the **Initiate tunneling** right to establish the tunnel connection for VNC.
- Port for tunneling RDP connections is opened (the **Open port for tunneling RDP connections** option is enabled in the **Connection ports** section of the Administration Server properties window).

*To connect to a Linux-based managed device by using VNC through Kaspersky Security Center Web Console opened on a Windows-based device:*

1. In the main menu, go to the **Asset management** → **Managed devices** section or open a device selection.
2. Select the check box next to the managed device to which you want to connect remotely, and then click the **Connect to Remote Desktop** button.

   The **Connect to Remote Desktop** window opens.

   If you select multiple devices, a mobile device, or a device running macOS, the **Connect to Remote Desktop** button will be disabled.
3. In the **Connect to Remote Desktop** window, select the connection type **VNC**.
4. Download the klsctunnel utility by clicking the **Download** button, and then run it.

   If the utility file is unavailable for download, an error message is displayed. In this case, download the utility manually.
5. In the **Connect to Remote Desktop** window, specify the VNC connection port. The default port number is 5900.
6. Generate a text blob with encoded connection parameters by clicking the **Generate blob** button, and then copy and paste the text into the corresponding field in the klsctunnel utility.

   A blob contains the settings required to establish a connection between Administration Server and the managed device. A blob is valid for three minutes. If it has expired, generate a new blob.
7. In the klsctunnel utility, if you use a proxy server, specify the proxy server connection settings.

   To do this, select the **Use proxy server** check box, and then specify the connection settings.
8. Click the **Open port** button.

   The klsctunnel utility displays the address and port for the local connection of the VNC client.

The utility allows the remote user to close the tunnel connection. If the tunnel connection is closed, the current connection to the remote desktop is terminated.

9. Run a VNC client and connect it to the managed device by using the address and port provided by the klsctunnel utility.

The connection with the managed device is established. The desktop is available in the VNC client window.

# Remote access from a Windows-based device with Kaspersky Security Center Web Console to a Windows-based managed device

Remote desktop connection (RDP)

**Prerequisites**

Before you start, make sure that you have done the following:

- On the managed device running Windows, Network Agent version 13 or later is installed.
- The administrator has the **Start RDP sessions** right to establish RDP connections.
- Port for tunneling RDP connections is opened (the **Open port for tunneling RDP connections** option is enabled in the **Connection ports** section of the Administration Server properties window).
- A remote connection is allowed in the operating system settings of the managed device.

*To connect to a Windows-based managed device by using RDP through Kaspersky Security Center Web Console opened on a Windows-based device:*

1. In the main menu, go to the **Asset management** → **Managed devices** section or open a device selection.
2. Select the check box next to the managed device to which you want to connect remotely, and then click the **Connect to Remote Desktop** button.

   The **Connect to Remote Desktop** window opens.

   If you select multiple devices, a mobile device, or a device running macOS, the **Connect to Remote Desktop** button will be disabled.
3. In the **Connect to Remote Desktop** window, select the **Remote Desktop Connection** connection type.
4. If a remote connection is not allowed in the operating system settings of the managed device, allow the remote connection centrally by clicking the **Change settings** button.

   If the settings are applied correctly, a notification is displayed. Also, on the managed device, in the **Settings** → **System** → **Remote Desktop** section, the **Enable Remote Desktop** option is enabled.

   If the remote connection is allowed in the operating system settings of the managed device, the **Change settings** button is not displayed.
5. Download the klsctunnel utility by clicking the **Download** button, and then run it.

When downloading the utility, take into account the following:

- To get an up-to-date version of the klsctunnel utility, make sure that Administration Server has access to Kaspersky update servers.

  You can run the *Download updates to the Administration Server repository* task and select Kaspersky update servers as a source of updates. If the task finishes successfully, Administration Server has access to Kaspersky update servers.

- If the utility file is unavailable for download, an error message is displayed. In this case, download the utility manually, and then place it on the Administration Server device in the /var/opt/kaspersky/klnagent_srv directory.

6. Generate a text blob with encoded connection parameters by clicking the **Generate blob** button, and then copy and paste the text into the corresponding field in the klsctunnel utility.

   A blob contains the settings required to establish a connection between Administration Server and the managed device. A blob is valid for three minutes. If it has expired, generate a new blob.

7. In the klsctunnel utility, if you use a proxy server, specify the proxy server connection settings.

   To do this, select the **Use proxy server** check box, and then specify the connection settings.

8. Click the **Open port** button.

   The Remote Desktop Connection login window opens.

9. Specify the credentials of the account under which you are currently logged in to Kaspersky Security Center Web Console, and then connect to the managed device.

   The klsctunnel utility displays the address and port of the connection to the remote device.

   The utility allows the administrator to close the tunnel connection. If the tunnel connection is closed, the current connection to the remote desktop is terminated.

When connection to the device is established, the desktop is available in the Remote Desktop Connection window of Microsoft Windows.

Connection to the current remote desktop session of the user is established without the user's knowledge. Once the administrator connects to the session, the device user is disconnected from the session without notification.

Windows Desktop Sharing (WDS)

**Prerequisites**

Before you start, make sure that you have done the following:

- On the managed device running Windows, Network Agent version 13 or later is installed.
- The administrator has the **Connect to existing RDP sessions** right to establish the WDS connection.
- The license for Vulnerability and patch management is available.

- Microsoft Windows Vista or later is installed on the administrator's workstation. The type of operating system of the device hosting Administration Server imposes no restrictions on connection through Windows Desktop Sharing.

  Check whether the Windows Desktop Sharing feature is included in your Windows edition, and make sure that the CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} key exists in the Windows Registry.

- Microsoft Windows Vista or later is installed on the client device.

*To connect to a Windows-based managed device by using VNC through Kaspersky Security Center Web Console opened on a Windows-based device:*

1. In the main menu, go to the **Asset management** → **Managed devices** section or open a device selection.

2. Select the check box next to the managed device to which you want to connect remotely, and then click the **Connect to Remote Desktop** button.

   The **Connect to Remote Desktop** window opens.

   If you select multiple devices, a mobile device, or a device running macOS, the **Connect to Remote Desktop** button will be disabled.

3. In the **Connect to Remote Desktop** window, select the connection type **Windows Desktop Sharing**.

   If the Vulnerability and patch management license is not available, an error message is displayed.

4. Download the klsctunnel utility by clicking the **Download** button, and then run it.

   If the utility file is unavailable for download, an error message is displayed. In this case, download the utility manually.

5. In the list of available user sessions active on the selected device, select the session to which you want to connect.

   The remote user must allow the connection. If the remote user refuses to connect or if the remote user does not allow the connection during the timeout period, an error message is displayed.

6. Generate a text blob with encoded connection parameters by clicking the **Generate blob** button, and then copy and paste the text into the corresponding field in the klsctunnel utility.

   A blob contains the settings required to establish a connection between Administration Server and the managed device. A blob is valid for three minutes. If it has expired, generate a new blob.

7. In the klsctunnel utility, if you use a proxy server, specify the proxy server connection settings.

   To do this, select the **Use proxy server** check box, and then specify the connection settings.

8. Click the **Open port** button.

   The klsctunnel utility displays the address and port for the local connection of the VNC client.

   The utility allows the remote user to close the tunnel connection. If the tunnel connection is closed, the current connection to the remote desktop is terminated.

Desktop sharing starts in a new window. If you want to interact with the device, click the menu icon (  ) in the upper-left corner of the window, and then select **Interactive mode**.

# Mobile Device Management

Management of mobile device protection through Kaspersky Security Center is carried out by using the Mobile Device Management feature. You have to add a license key on each mobile device to activate the protection application. If you intend to manage mobile devices owned by employees in your organization, enable and configure Mobile Device Management.

Mobile Device Management enables you to manage Android and iOS devices of the employees. The protection is provided by the Kaspersky Endpoint Security for Android app and iOS device management system installed on the mobile devices. These mobile apps ensure protection of mobile devices against web threats, viruses, and other programs that pose threats. For centralized management through Kaspersky Security Center Web Console, you must install the following web management plug-ins on the device where Kaspersky Security Center Web Console is installed:

- Kaspersky Mobile Devices Protection and Management

  The Kaspersky Mobile Devices Protection and Management plug-in allows you to manage devices running Android and iOS in Kaspersky Security Center Web Console.

- iOS MDM Server settings

  The iOS MDM Server settings plug-in allows you to configure the settings of the iOS MDM server that is used to connect iOS devices to the Administration Server and manage iOS devices.

For information about protection deployment and management of mobile devices, see Kaspersky Security for Mobile Help and Kaspersky Secure Mobility Management Help.

# Using Firebase Cloud Messaging

To ensure timely delivery of commands to Android devices, Kaspersky Security Center Linux uses the mechanism of push notifications. Push notifications are exchanged between Android devices and Administration Server through Firebase Cloud Messaging (hereinafter referred to as FCM). In Kaspersky Security Center Linux Web Console, you can specify the Firebase Cloud Messaging settings to connect Android devices to the service.

To retrieve the settings of Firebase Cloud Messaging, you must have a Google account.

*To enable the use of FCM:*

1. In the main window of Kaspersky Security Center Web Console, select **Asset management** → **Mobile** → **Devices**.

2. Open the 3-dot menu ( ⋮ ) and select **Forced Android device synchronization**.

3. In the **Firebase project number** field, specify the FCM Sender ID.

4. In the **Private key** field, select the private key file.

   At the next synchronization with Administration Server, Android devices will be connected to Firebase Cloud Messaging.

When you switch to a different Firebase project, you need to wait 10 minutes for FCM to resume.

FCM service runs in the following address ranges:

- From the Android device's side, access is required to ports 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS), and 5230 (HTTPS) of the following addresses:
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - All of the IP addresses listed in Google's ASN of 15169
- From the Administration Server side, access is required to port 443 (HTTPS) of the following addresses:
  - fcm.googleapis.com
  - All of the IP addresses listed in Google's ASN of 15169

If the proxy server settings have been specified in the Administration Server properties in Kaspersky Security Center Web Console, they will be used for interaction with FCM.

When changing the `strDeviceRegId` value for a device in the gcm_devices table in the server part of FCM, synchronization of the changed value with the server part of Kaspersky Security Center takes 5 minutes. During synchronization, messages may be received on the device for which the `strDeviceRegId` value has been changed with a delay.

### Configuring FCM: getting the Sender ID and private key file

*To configure FCM:*

1. Register on the Google portal.
2. Go to the Firebase console.
3. Do one of the following:
   - To create a new project, click **Create a project** and follow the instructions on the screen.
   - Open an existing project.

4. Click the gear icon and choose **Project settings**.

   The **Project settings** window opens.

5. Select the **Cloud Messaging** tab.

6. Retrieve the relevant Sender ID from the **Sender ID** field in the **Firebase Cloud Messaging API (V1)** section.

7. Select the **Service accounts** tab and click **Generate new private key**.

8. In the window that opens, click **Generate key** to generate and download a private key file.

Firebase Cloud Messaging is now configured.

# Integration with Public Key Infrastructure

You can integrate the issuance of certificates with Microsoft Certification Authority (CA) via Public Key Infrastructure (PKI). Integration with PKI is intended for simplifying the issuance of domain user certificates by Administration Server. Following integration, certificates are issued automatically.

For detailed information on configuring integration with PKI to issue certificates, refer to the Kaspersky Secure Mobility Management Help.

You can perform the PKI integration with specified settings and assign PKI to act as the source of certificates for specific types of certificates. The PKI integration settings allow you to set the individual default template for all types of certificates.

The specifics of using PKI integration to issue certificates:

- PKI integration is disabled by default. For detailed information on enabling PKI and configuring its settings, refer to the Kaspersky Secure Mobility Management Help.

- Certificates are issued using Network Agent for Windows. This ensures integration between the Administration Server and Microsoft CA. Since there can be multiple devices with Network Agent installed, you can specify the device that will connect to Microsoft CA in the **Issuance rules**. This device must have an Enrollment Agent (EA) certificate installed in the certificates repository of the account under which the integration with PKI is performed. The certificate is issued by the administrator of the domain's CA.

- The account under which integration with PKI is performed must be a domain user and have the right to *Log On As Service*.

- Kaspersky Security Center Linux can only work with one PKI (Microsoft CA) integration at a time.

# Managing administration groups

This section provides information about how to manage administration groups.

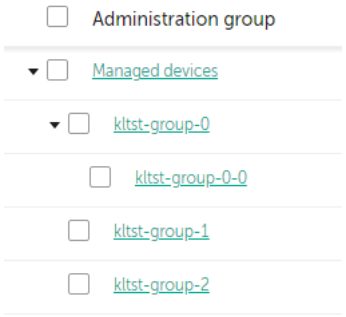
You can perform the following actions on administration groups:

- Add any number of nested groups at any level of hierarchy to administration groups.
- Add devices to administration groups.
- Change the hierarchy of administration groups by moving individual devices and entire groups to other groups.
- Remove nested groups and devices from administration groups.
- Add secondary and virtual Administration Servers to administration groups.
- Move devices from the administration groups of an Administration Server to those of another Server.
- Define which Kaspersky applications will be automatically installed on devices included in a group.

You can perform these actions only if you have the **Modify** permission in the **Management of administration groups** area for the administration groups you want to manage (or for the Administration Server to which these groups belong).

# Creating administration groups

Immediately after Kaspersky Security Center installation, the hierarchy of administration groups contains only one administration group called **Managed devices**. When creating a hierarchy of administration groups, you can add devices and virtual machines to the **Managed devices** group, and add nested groups (see the figure below).

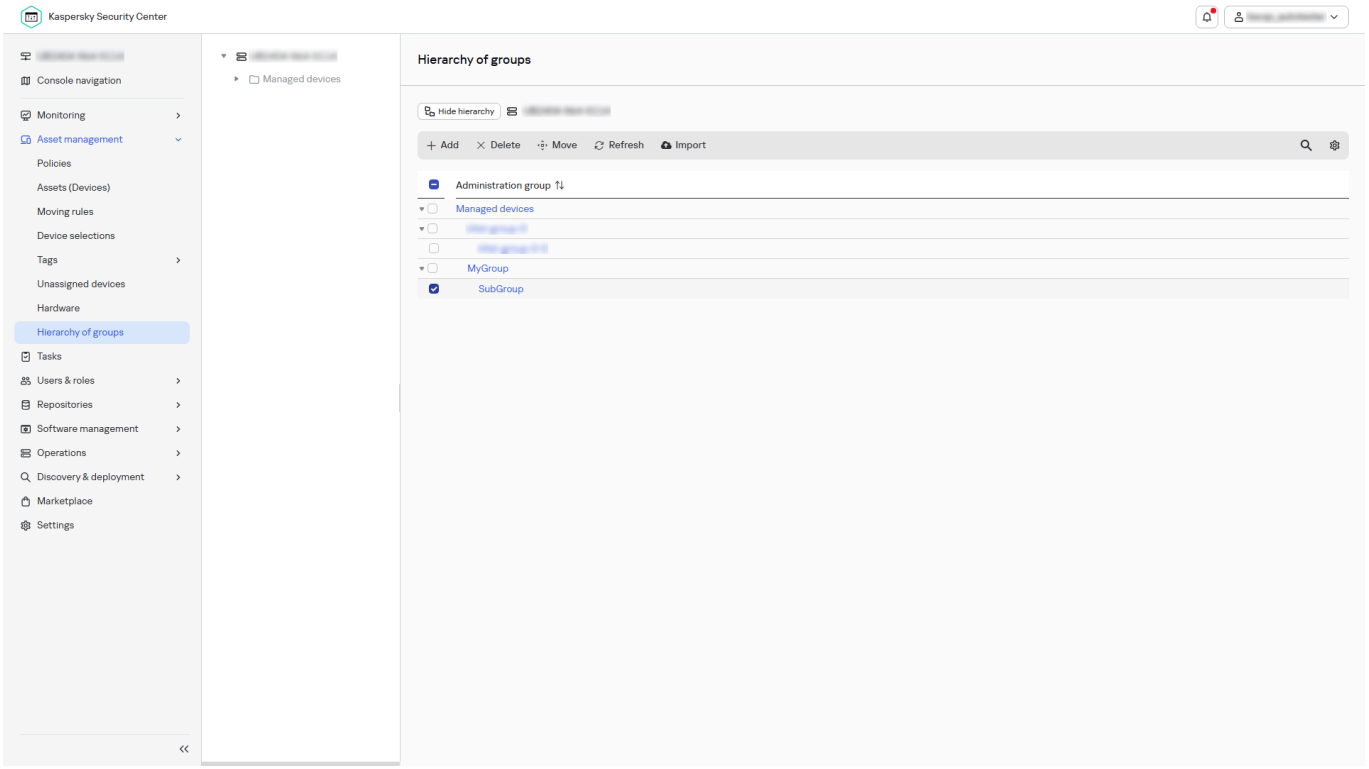



Viewing administration groups hierarchy

*To create an administration group:*

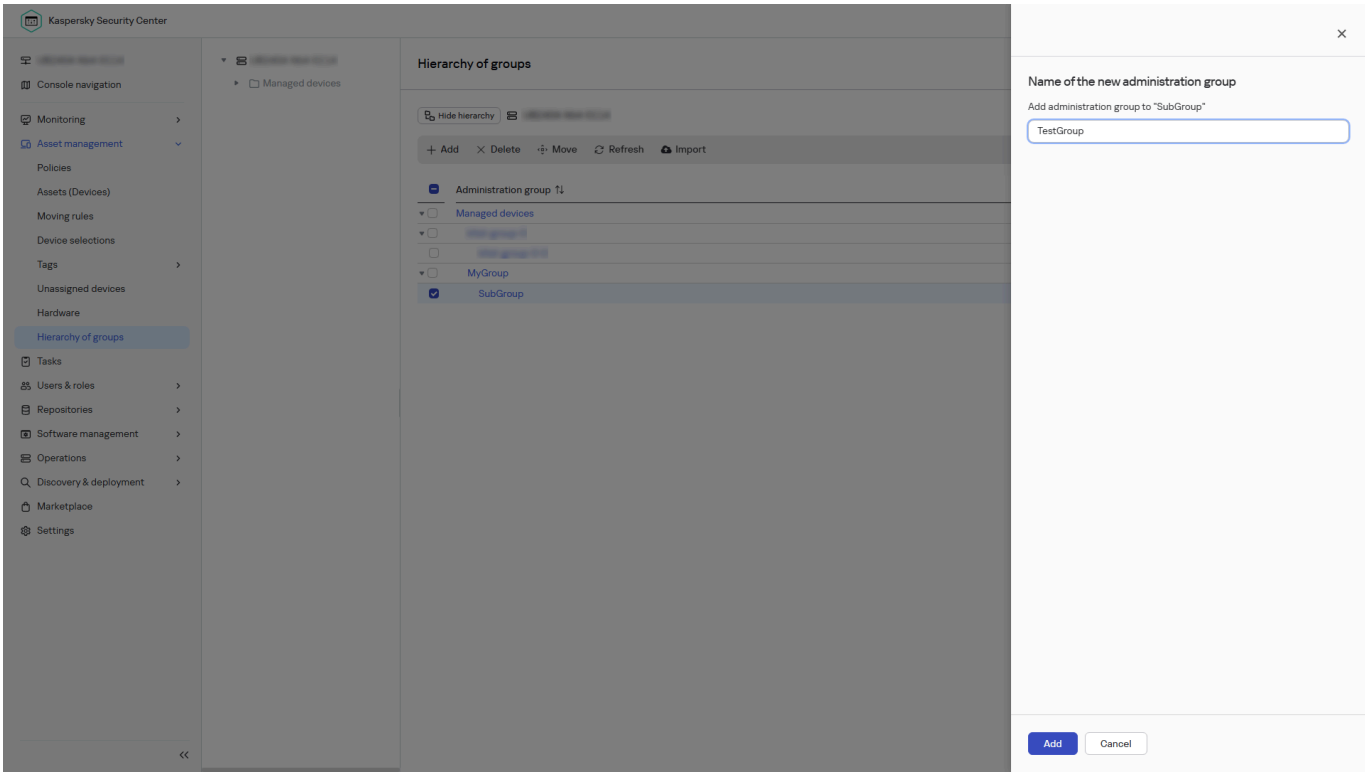
1. In the main menu, go to **Asset management** → **Hierarchy of groups**.

2. In the administration group structure, select the administration group that is to include the new administration group.




3. Click **Add**.

4. In the **Name of the new administration group** window that opens, enter a name for the group, and then click the **Add** button.




A new administration group with the specified name appears in the hierarchy of administration groups.

*To create a structure of administration groups:*

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. Click **Import**.

The New Administration Group Structure Wizard starts. Follow the steps of the wizard.

# Automatic installation of applications on devices in an administration group

You can specify which installation packages must be used for automatic remote installation of Kaspersky applications to client devices in an administration group.

*To configure automatic installation of applications on the devices in an administration group:*

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. Go to the properties of the required administration group in one of the following ways:
   - Click the name of the administration group.
   - Click the **Show hierarchy** button at the top of the page. In the navigation pane that opens, hover the mouse cursor over the name of the required group, and then click the settings icon ( ⚙ ).

   The administration group properties window opens.
3. In the properties window, go to the **Automatic installation** tab.
4. Select the installation packages of the applications to be installed on the devices, and then click the **Save** button.

   If you select several installation packages of the same application that differ only in their versions, the installation package with the latest version is saved.

After you select the installation packages, a group tasks for installation of the applications on the devices in the administration group is created for each of the application. These tasks are run on the client devices immediately after they are added to the administration group.

# Moving administration groups

You can move nested administration groups within the groups hierarchy.

An administration group is moved together with all nested groups, secondary Administration Servers, devices, group policies, and tasks. The system will apply to the group all the settings that correspond to its new position in the hierarchy of administration groups.

The name of the group must be unique within one level of the hierarchy. If a group with the same name already exists in the folder into which you move the administration group, you should change the name of the latter. If you have not changed the name of the moved group, an index in **(<next sequence number>)** format is automatically added to its name when it is moved, for example: **(1)**, **(2)**.

You cannot rename and move the **Managed devices** group.

*To move an administration group to another level of the administration groups hierarchy:*

1. In the main menu, go to **Asset management** → **Hierarchy of groups**, and then select the check box next to the administration group that you want to move.
2. Click the **Move** button on the toolbar.
3. In the window that opens, select where you want to move the administration group, and then click the **Move** button.

The window is closed, and the administration group is moved to another level of the groups hierarchy.

# Deleting administration groups

If you delete an administration group that contains secondary Administration Servers, nested groups, client devices, group tasks, or policies created for this group, all of them will also be deleted.

Before deleting an administration group, you must delete all secondary Administration Servers, nested groups, and client devices from that group.

*To delete an administration group:*

1. In the main menu, go to **Asset management** → **Hierarchy of groups**, and then select the check box next to the administration group that you want to delete.
2. Click the **Delete** button on the toolbar.

The administration group is deleted.

# Deploying Kaspersky applications

This section describes Kaspersky applications deployment on client devices in your organization by means of Kaspersky Security Center Web Console.

# Scenario: Kaspersky applications deployment

This scenario explains how to deploy Kaspersky applications through Kaspersky Security Center Web Console. You can use the quick start wizard and Protection deployment wizard, or you can complete all necessary steps manually.

The following applications are available for deployment by using Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

## Stages

Kaspersky applications deployment proceeds in stages:

1. **Downloading management web plug-in for the application**

   This stage is handled by the quick start wizard. If you choose not to run the wizard, download the plug-ins manually.

2. **Downloading and creating installation packages**

   This stage is handled by the quick start wizard.

   The quick start wizard allows you to download the installation package with the management web plug-in. If you did not select this option when running the wizard, or if you did not run the wizard at all, you must download the package manually.

   If you cannot install Kaspersky applications by means of Kaspersky Security Center Linux on some devices, for example, on remote employees' devices, you can create stand-alone installation packages for applications. If you use stand-alone packages to install Kaspersky applications, you do not have to create and run a remote installation task, nor create and configure tasks for Kaspersky Endpoint Security for Windows.

   Alternatively, you can download the distribution packages for Network Agent and security applications from the Kaspersky website. If the remote installation of the applications is not possible for some reason, you can use the downloaded distribution packages to install the applications locally.

3. **Creating, configuring, and running the remote installation task**

   This step is part of the Protection deployment wizard. If you choose not to run the Protection deployment wizard, you must create this task manually and configure it manually.

   You also can manually create several remote installation tasks for different administration groups or different device selections. You can deploy different versions of one application in these tasks.

   Make sure that all the devices on your network are discovered; then run the remote installation task (or tasks).

If you want to install Network Agent on devices with the SUSE Linux Enterprise Server 15 operating system, install the insserv-compat package first to configure Network Agent.

If you want to install Network Agent on devices that use the operating system RED OS 7.3.4 or later or MSVSPHERE 9.2 or later, install the libxcrypt-compat package for the correct function of Network Agent.

4. **Creating and configuring tasks**

   The *Update* task of Kaspersky Endpoint Security must be configured.

   This step is part of the quick start wizard: the task is created and configured automatically with the default settings. If you did not run the wizard, you must create this task manually and configure it manually. If you use the quick start wizard, make sure that the schedule for the task meets your requirements. (By default, the scheduled start for the task is set to **Manually**, but you might want to choose another option.)

5. **Creating policies**

   Create the policy for Kaspersky Endpoint Security manually or through the quick start wizard. You can use the default policy settings. You can also modify the default settings of the policy in accordance with your needs at any time.

6. **Verifying the results**

   Make sure that deployment was completed successfully: you have policies and tasks for each application, and these applications are installed on the managed devices.

Results

Completion of the scenario yields the following:

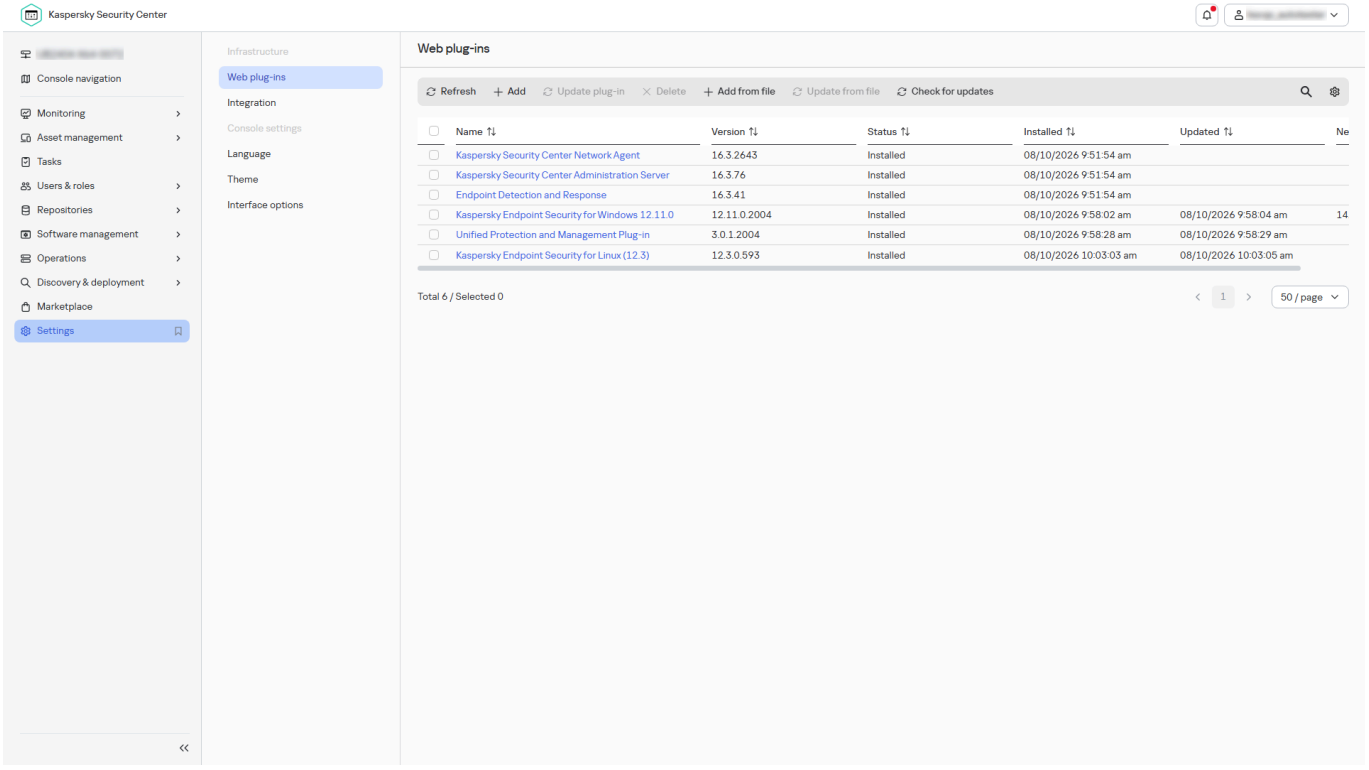
- All required policies and tasks for the selected applications are created.
- The schedules of tasks are configured according to your needs.
- The selected applications are deployed, or scheduled to be deployed, on the selected client devices.

# Adding management plug-ins for Kaspersky applications

To deploy a Kaspersky application, for example, Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Windows, you must add and install the management web plug-in for the application.

*To download a management web plug-in for a Kaspersky application:*

1. In the main menu, go to the **Settings** → **Web plug-ins**.




The list of installed web plug-ins

2. In the window that opens, click the **Add** button.

   The list of available plug-ins is displayed.

3. In the list of available plug-ins, select the plug-in you want to download (for example, Kaspersky Endpoint Security for Linux) by clicking on its name.

   A plug-in description page is displayed.

4. On the plug-in description page, click **Install plug-in**.

5. When the installation is complete, click **OK**.

The management web plug-in is downloaded with the default configuration and displayed in the list of management web plug-ins.

You can add plug-ins and update downloaded plug-ins from a file. You can download management web plug-ins from the Kaspersky website.

*To download or update management web plug-in from a file:*

1. In the main menu, go to the **Settings** → **Web plug-ins**.

2. Specify the file of the plug-in and the signature of the file:

   - Click **Add from file** to download a plug-in from a file.

   - Click **Update from file** to download an update of a plug-in from a file.

3. Specify the file and signature of the file.

4. Download the specified files.

The management web plug-in is downloaded from the file and displayed in the list of management web plug-ins.

# Packages

*Installation package* is a set of files created for remote installation of a Kaspersky application. The installation package contains a range of settings needed to install the application and get it running immediately after installation. Settings correspond to application defaults. The installation package is created using files with the KPD and KUD extensions included in the application distribution kit.

Installation packages are generated by using the following methods:

- Automatically, from specified distribution packages, on the basis of included *descriptors* (files with the kud extension that contain rules for installation and results analysis, and other information).
- From a ZIP, CAB, TAR, or TAR.GZ archive file, for standard or supported applications.

Generated installation packages are organized hierarchically as folders with subfolders and files. In addition to the original distribution package, an installation package contains editable settings (including the installer's settings and rules for processing such cases as necessity of restarting the operating system in order to complete installation), as well as minor auxiliary modules.

Values of installation settings that would be specific for an individual supported application can be defined in the user interface of Kaspersky Security Center Web Console when the installation package is created. When performing remote installation of applications through Kaspersky Security Center Linux tools, installation packages are delivered to devices so that running the installer of an application makes all administrator-defined settings available for that application. When using third-party tools for installation of Kaspersky applications, you only have to ensure the availability of the entire installation package on the device, that is, the availability of the distribution package and its settings. Installation packages are created and stored by Kaspersky Security Center Linux in a dedicated subfolder of the shared folder.

Do not specify any details of privileged accounts in the parameters of installation packages.

Deployment using group policies of Microsoft Windows is not supported.

Immediately after Kaspersky Security Center Linux installation, a few installation packages are automatically generated; they are ready for installation and include Network Agent packages and security application packages for Microsoft Windows.

Although the license key for an application can be set in the properties of an installation package, it is advisable to avoid this method of license distribution because there it is easy to obtain read access to installation packages. You should use automatically distributed license keys or installation tasks for license keys.

# Downloading and creating installation packages for Kaspersky applications

You can create installation packages for Kaspersky applications from Kaspersky web servers if your Administration Server has access to the internet.

When creating installation packages for installing the application on Windows devices, if you get the message **Error has occurred. Please retry download**:

1. Create the RIUtilsArchiveDirUsed flag by running the following command:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Run the following command to restart the Administration Server service:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Download additional modules, "Files for remote installation via Kaspersky Security Center" from the Kaspersky website.

   The downloaded archives have the following names:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Do not rename the archives.

4. Place the archives in the /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives directory.

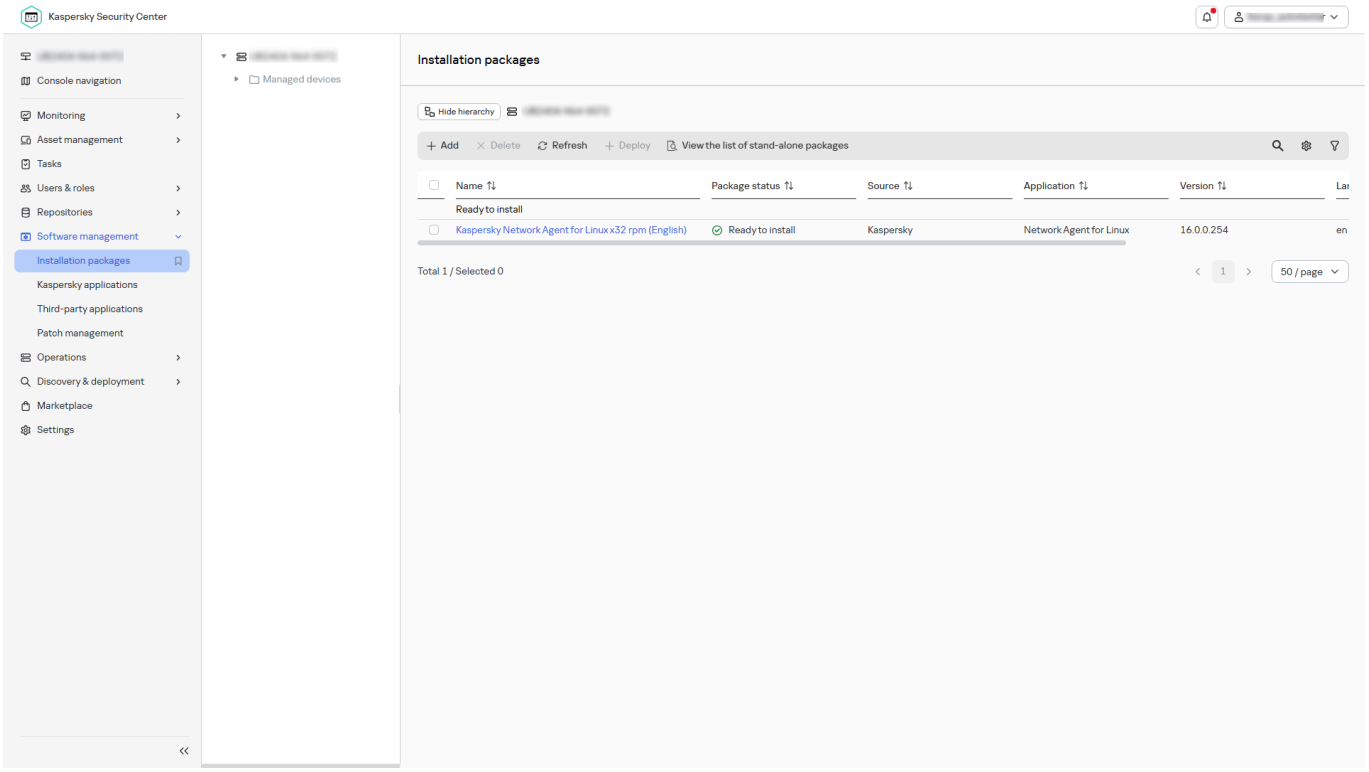
Now you can create an installation package for installing the application on Windows devices.

*To download and create installation package for Kaspersky application:*

1. In the main menu, go to **Software management** → **Installation packages**.

   You can also view notifications about new packages for Kaspersky applications in the list of onscreen notifications. If there are notifications about a new package, you can click the link next to the notification and proceed to the list of available installation packages.

A list of installation packages available on Administration Server is displayed.

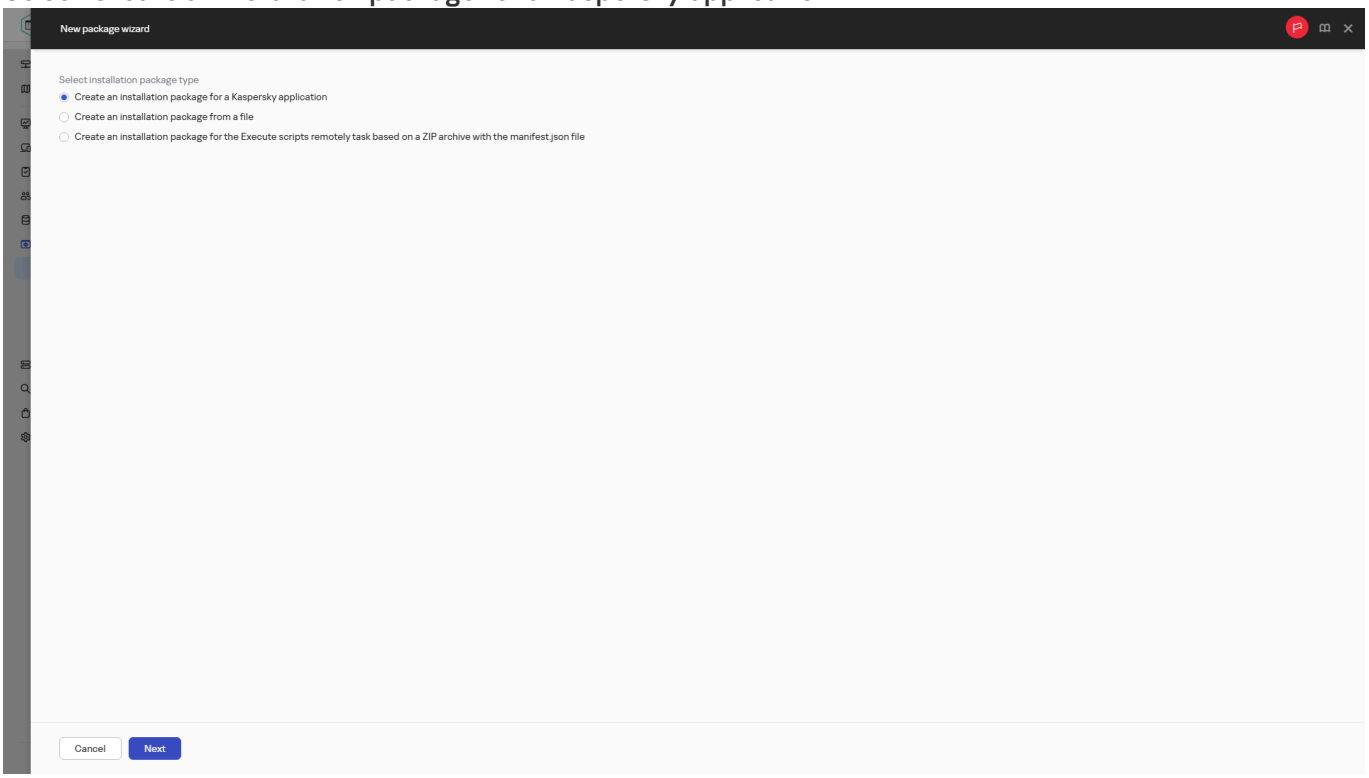



The list of installation packages

2. Click **Add**.

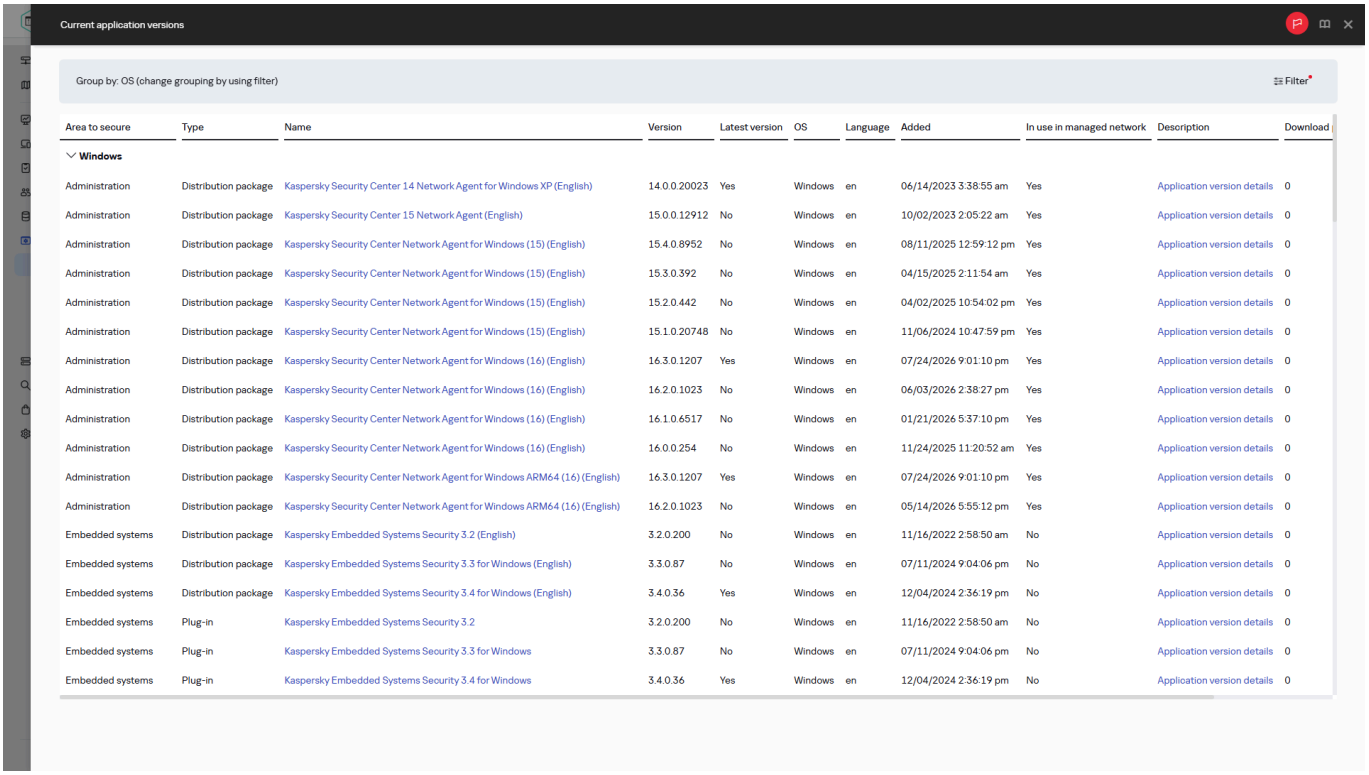
   The New package wizard starts. Proceed through the wizard by using the **Next** button.

3. Select **Create an installation package for a Kaspersky application**.




Selecting the installation package type

A list of available installation packages on Kaspersky web servers appears. The list contains installation packages only for those applications that are compatible with the current version of Kaspersky Security Center Linux. By default, the list only shows applications with the English language and the language that matches the interface language. To display other languages, click **Filter** and configure the filter settings.



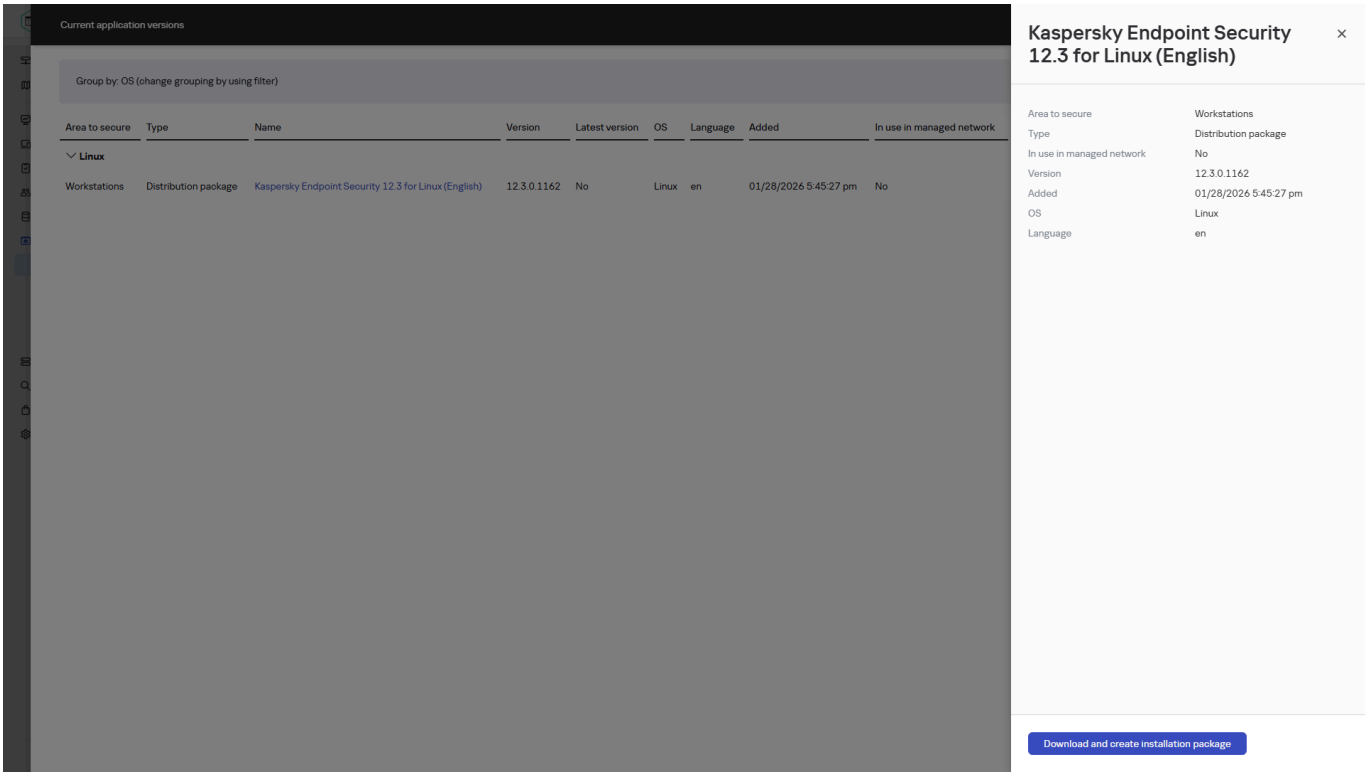

| Area to secure | Type | Name | Version | Latest version | OS | Language | Added | In use in managed network | Description | Download |
|---|---|---|---|---|---|---|---|---|---|---|
| Windows | | | | | | | | | | |
| Administration | Distribution package | Kaspersky Security Center 14 Network Agent for Windows XP (English) | 14.0.0.20023 | Yes | Windows | en | 06/14/2023 3:38:55 am | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center 15 Network Agent (English) | 15.0.0.12912 | No | Windows | en | 10/02/2023 2:05:22 am | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (15) (English) | 15.4.0.8952 | No | Windows | en | 08/11/2025 12:59:12 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (15) (English) | 15.3.0.392 | No | Windows | en | 04/15/2025 2:11:54 am | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (15) (English) | 15.2.0.442 | No | Windows | en | 04/02/2025 10:54:02 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (15) (English) | 15.1.0.20748 | No | Windows | en | 11/06/2024 10:47:59 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (16) (English) | 16.3.0.1207 | Yes | Windows | en | 07/24/2026 9:01:10 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (16) (English) | 16.2.0.1023 | No | Windows | en | 06/03/2026 2:38:27 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (16) (English) | 16.1.0.6517 | No | Windows | en | 01/21/2026 5:37:10 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows (16) (English) | 16.0.0.254 | No | Windows | en | 11/24/2025 11:20:52 am | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows ARM64 (16) (English) | 16.3.0.1207 | Yes | Windows | en | 07/24/2026 9:01:10 pm | Yes | Application version details | 0 |
| Administration | Distribution package | Kaspersky Security Center Network Agent for Windows ARM64 (16) (English) | 16.2.0.1023 | No | Windows | en | 05/14/2026 5:55:12 pm | Yes | Application version details | 0 |
| Embedded systems | Distribution package | Kaspersky Embedded Systems Security 3.2 (English) | 3.2.0.200 | No | Windows | en | 11/16/2022 2:58:50 am | No | Application version details | 0 |
| Embedded systems | Distribution package | Kaspersky Embedded Systems Security 3.3 for Windows (English) | 3.3.0.87 | No | Windows | en | 07/11/2024 9:04:06 pm | No | Application version details | 0 |
| Embedded systems | Distribution package | Kaspersky Embedded Systems Security 3.4 for Windows (English) | 3.4.0.36 | Yes | Windows | en | 12/04/2024 2:36:19 pm | No | Application version details | 0 |
| Embedded systems | Plug-in | Kaspersky Embedded Systems Security 3.2 | 3.2.0.200 | No | Windows | en | 11/16/2022 2:58:50 am | No | Application version details | 0 |
| Embedded systems | Plug-in | Kaspersky Embedded Systems Security 3.3 for Windows | 3.3.0.87 | No | Windows | en | 07/11/2024 9:04:06 pm | No | Application version details | 0 |
| Embedded systems | Plug-in | Kaspersky Embedded Systems Security 3.4 for Windows | 3.4.0.36 | Yes | Windows | en | 12/04/2024 2:36:19 pm | No | Application version details | 0 |

The list of available installation packages

4. Click the name of an installation package, for example, Kaspersky Endpoint Security for Linux.

   A window opens with information about the installation package.

You can download and use an installation package which includes cryptographic tools that implement strong encryption, if it complies with applicable laws and regulations. To download the installation package of Kaspersky Endpoint Security for Windows valid for the needs of your organization, consult the legislation of the country where the client devices of your organization are located.




Downloading the installation package

5. Read the information and click the **Download and create installation package** button.

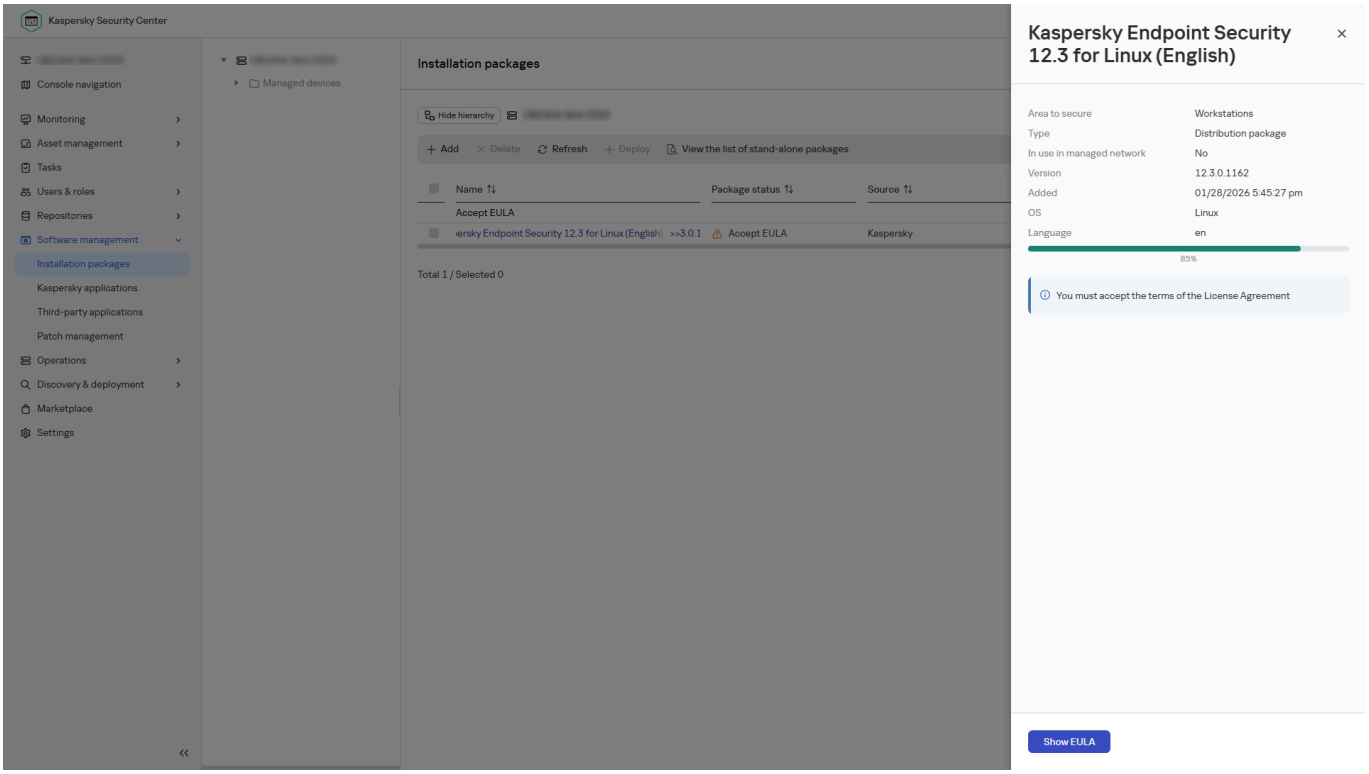
   If a distribution package can not be converted to an installation package, the **Download and create installation package** button instead of the **Download distribution package** is displayed.

For some Kaspersky applications, before or during the download process the **Show EULA** button is displayed. If it is displayed, do the following:

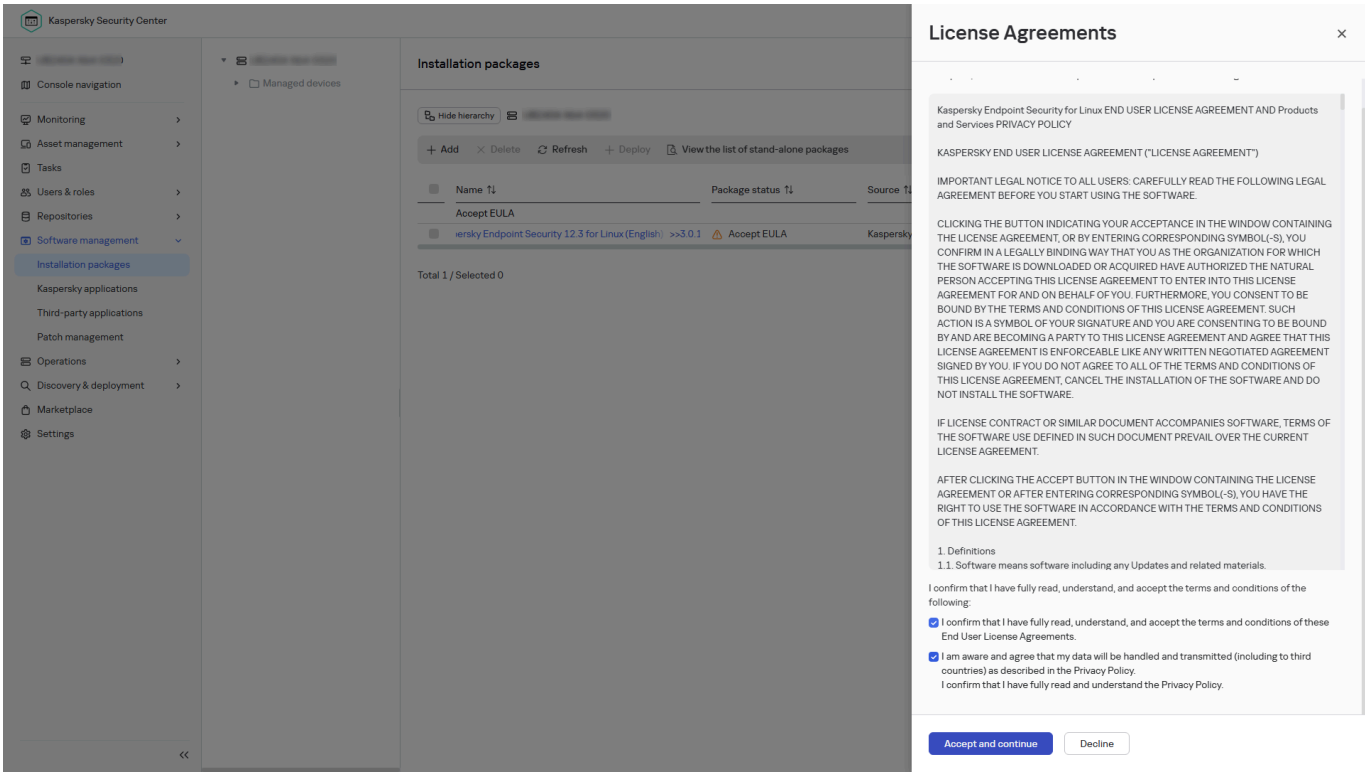
a. Click the **Show EULA** to read the End User License Agreement (EULA).

b. Read the EULA that is displayed on the screen, and click **Accept**.

The downloading continues after you accept the EULA. If you click **Decline**, the download is stopped.




Downloading the installation package




Accepting the EULA

You can close the wizard's window. In this case, the download process will continue in background mode. You can track the installation package download status as well as filter and sort the statuses in the **Package status** column.

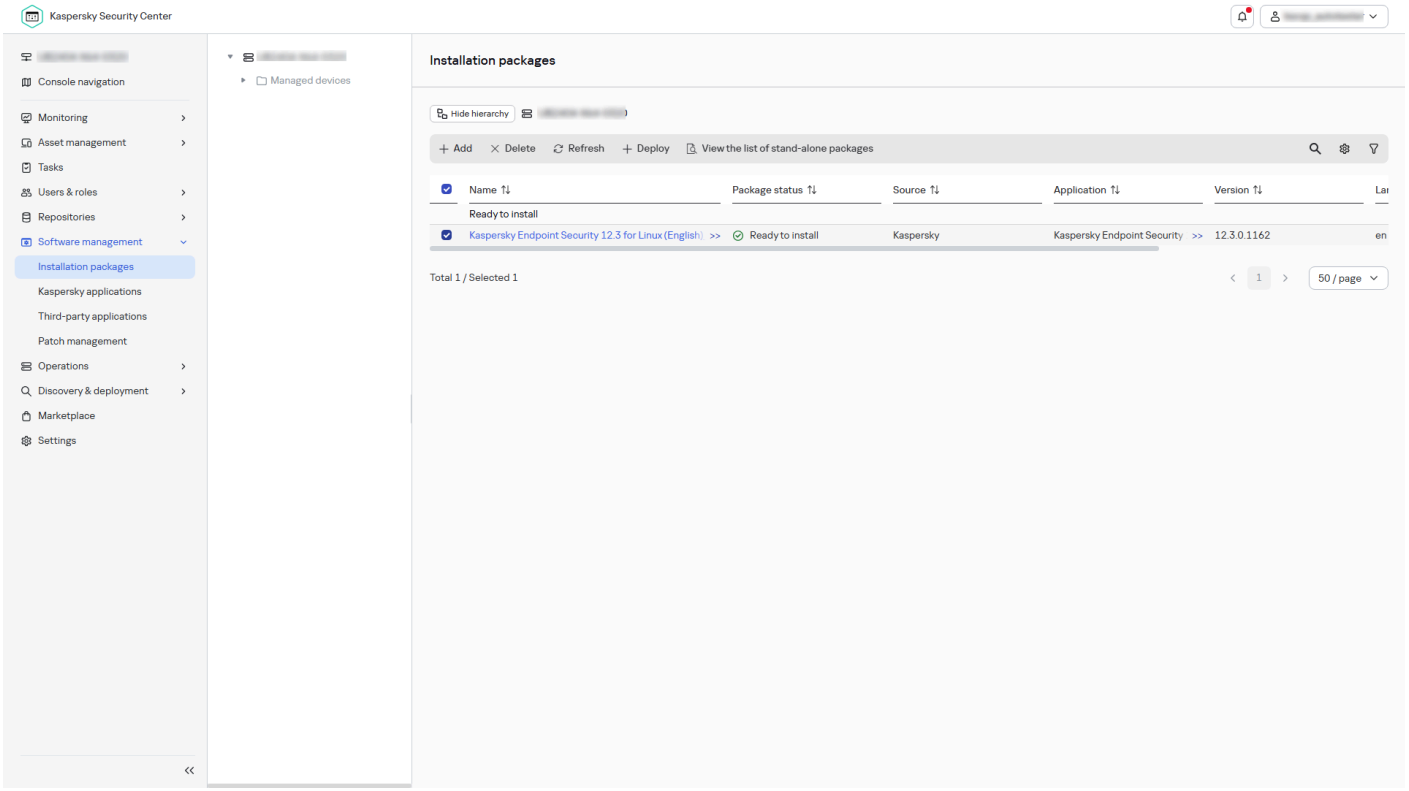
If the download process stops and the download status switches to **Accept EULA**, then click the installation package name and perform steps 5.a and 5.b.

By default, the installation packages with **In progress** and **Accept EULA** statuses are placed at the beginning of the list.

If the size of data contained in the selected distribution package exceeds the current limit, an error message is displayed. You can change the limit value and then proceed with the installation package creation.

6. When the downloading is complete, click the **Close** button.

The selected installation package is downloaded to the Administration Server shared folder, to the Packages subfolder. After downloading, the installation package is displayed in the list of installation packages.




The list of installation packages

# Creating installation packages from a file

You can use custom installation packages to do the following:

- To install any application (such as a text editor) on a client device, for example, by means of a task.
- To create a stand-alone installation package.

A custom installation package is a folder with a set of files. The source to create a custom installation package is an *archive file*. The archive file contains a file or files that must be included in the custom installation package.

If the Administration Server has access to the repository of application distribution packages for remote installation, use the **Download updates to the Administration Server repository** task to download the dependencies required to create installation packages for installing applications on Windows devices.

If the Administration Server does not have access to the repository of application distribution packages for remote installation:

1. Create the RIUtilsArchiveDirUsed flag by running the following command:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Download additional modules, "Files for remote installation via Kaspersky Security Center" from the Kaspersky website.

   The downloaded archives have the following names:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Do not rename the archives.

3. Place the archives in the /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives directory.

   Otherwise, when creating an installation package, the following error is displayed: **Remote installation utilities for win32 not found**.

4. Run the following command to restart the Administration Server service:

   ```
   systemctl restart kladminserver_srv.service
   ```

The Administration Server now has the required dependencies.

While creating a custom installation package, you can specify command-line parameters, for example, to install the application in silent mode.

Watch the video to learn how to create and deploy a custom installation package for Windows. The text version of this tutorial for both Windows and Linux devices is available below.

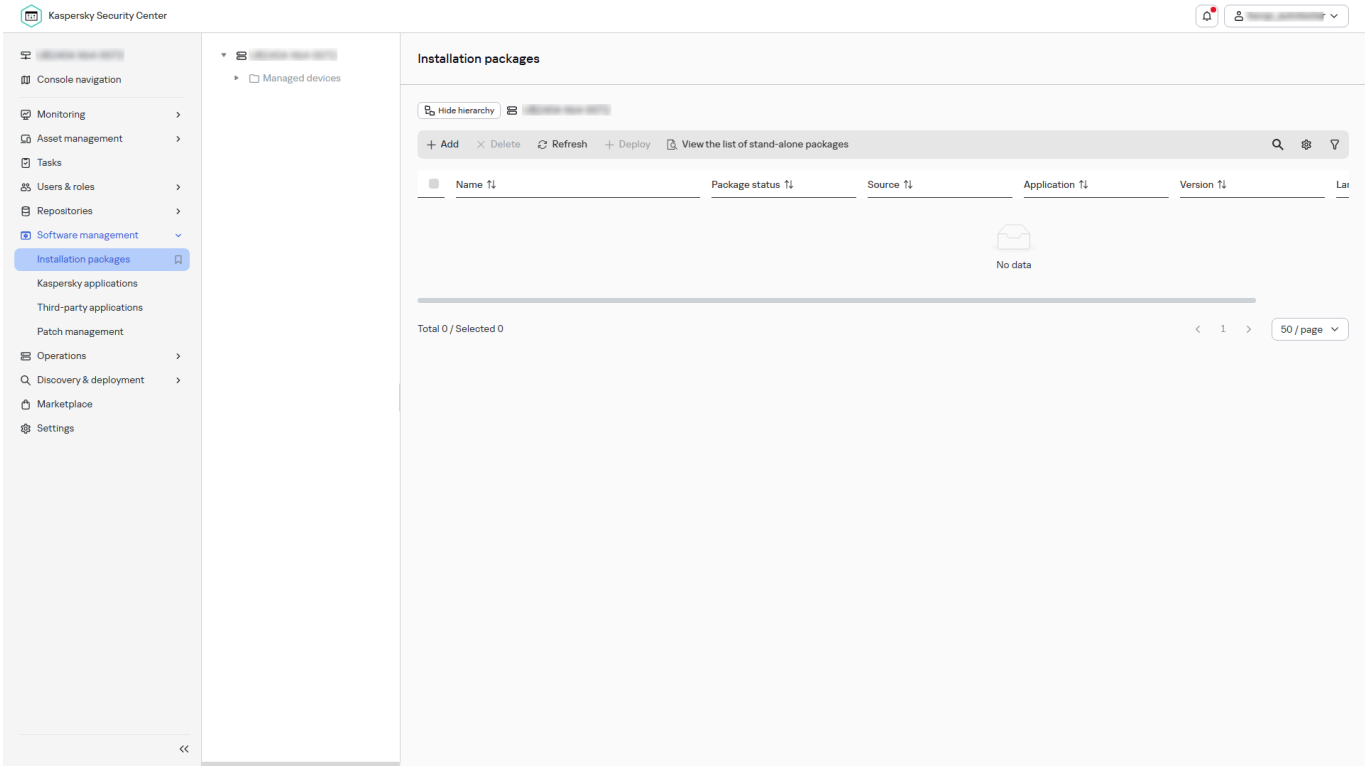



Creating and deploying a custom installation package from a file for Windows. Video

*To create a custom installation package:*

1. In the main menu, go to **Software management** → **Installation packages**.

   A list of installation packages available on the Administration Server is displayed.

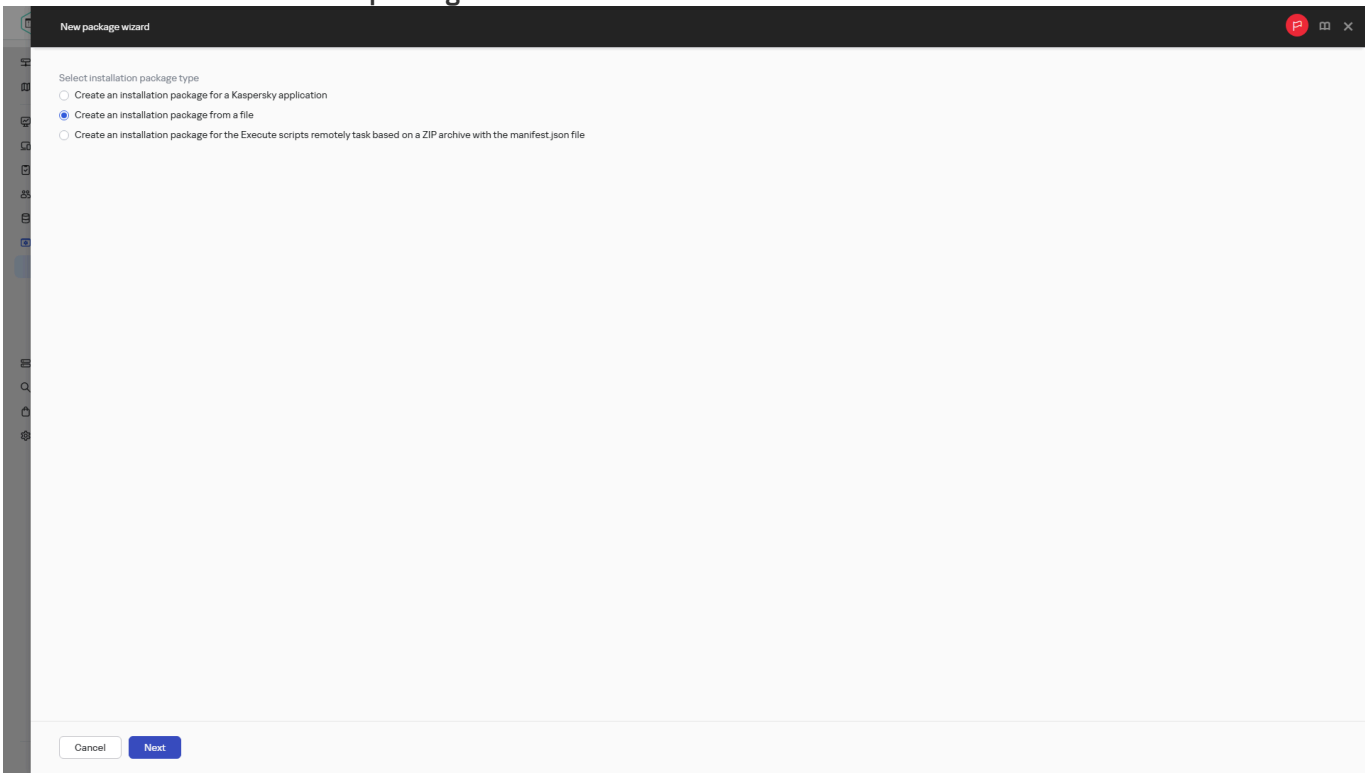



The list of installation packages

2. Click **Add**.

   The New package wizard starts. Proceed through the wizard by using the **Next** button.

3. Select **Create an installation package from a file**.



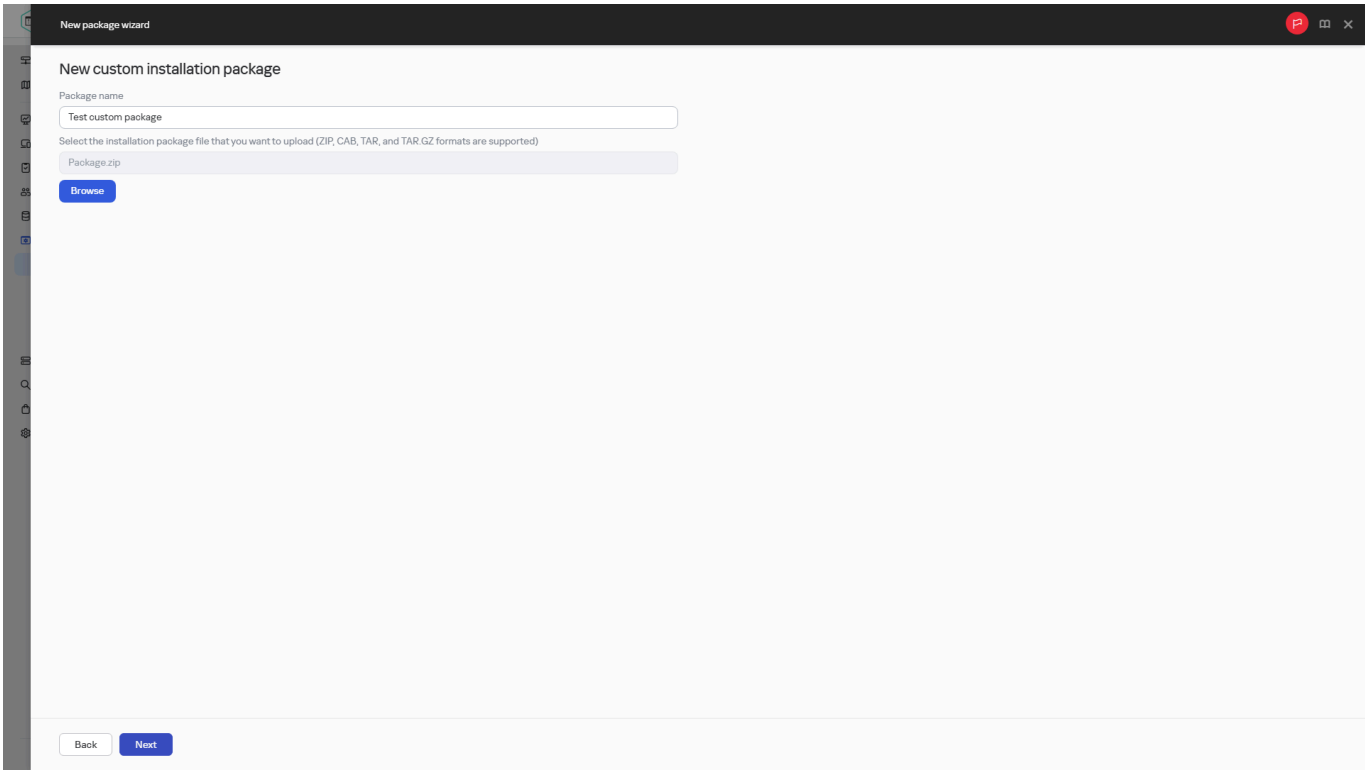

Selecting the installation package type

4. Specify the package name and click the **Browse** button.

5. In the window that opens, choose an archive file located on the available disks.

   You can upload a ZIP, CAB, TAR, or TAR.GZ archive file. It is not possible to create an installation package from an SFX (self-extracting archive) file.

   File upload to the Administration Server starts.




Specifying the installation package file

6. If you specified a file of a Kaspersky application, you may be prompted to read and accept the End User License Agreement (EULA) for the application. To continue, you must accept the EULA. Select the **Accept the terms and conditions of this End User License Agreement** option only if you have fully read, understand and accept the terms of the EULA.

   Additionally, you may be prompted to read and accept the Privacy Policy. To continue, you must accept the Privacy Policy. Select the **I accept the Privacy Policy** option only if you understand and agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy.

7. Select a file (from the list of files that are extracted from the chosen archive file) and specify the command-line parameters of an executable file.

   **How to create an installation package in deb or rpm format**

   1. Create a `.sh` script with the following commands:

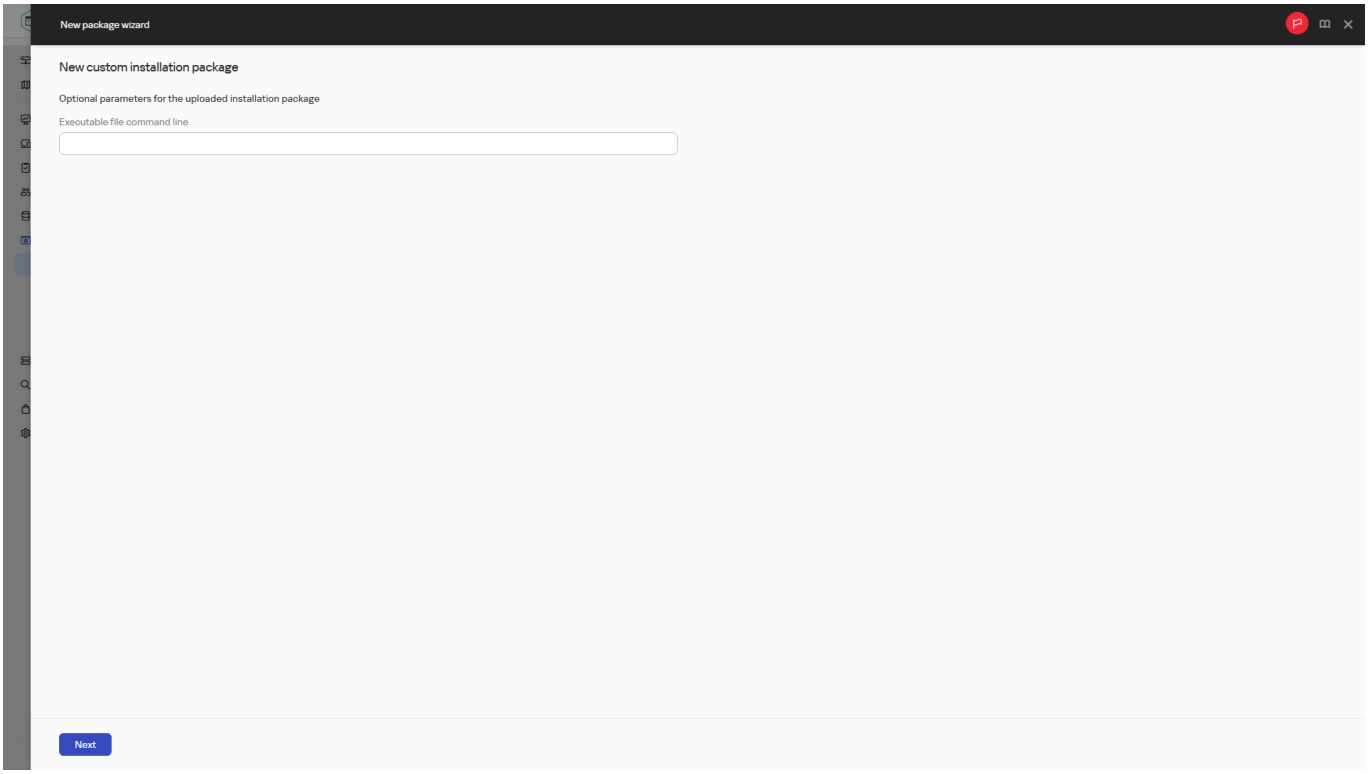
      ```
      #!/bin/sh
      script_dir="$(dirname "$0")"
      apt-get install --yes "$script_dir/<package_name>.deb" </dev/null
      ```

      The script content and commands may vary depending on the package format and other details. You can modify the script to suit your specific configuration.

   2. Place the created script in an archive, along with the `.deb` or `.rpm` file.

   3. When creating the installation package, select the created script as the executable file.

You can specify command-line parameters to install the application from the installation package in a silent mode. Specifying command-line parameters is optional.




Specifying the optional command-line parameters

The process to create the installation package is started.

The wizard informs you when the process is finished.

If the installation package is not created, an appropriate message is displayed.

8. Click the **Finish** button to close the wizard.

The installation package that you created is downloaded to the Packages subfolder of the Administration Server shared folder. After downloading, the installation package appears in the list of installation packages.

In the list of installation packages available on Administration Server, by clicking the link with the name of a custom installation package, you can:

- View the following properties of an installation package:
  - **Name**. Custom installation package name.
  - **Package status**. Installation package download status.
  - **Source**. Application vendor name.
  - **Application**. Application name packed into the custom installation package.
  - **Version**. Application version.
  - **Language**. Language of the application packed into the custom installation package.
  - **Size (MB)**. Size of the installation package.
  - **OS**. Type of the operating system for which the installation package is intended.

- **Created**. Installation package creation date.
- **Modified**. Installation package modification date.
- **Type**. Type of the installation package.

- Change the command-line parameters.

# Creating stand-alone installation packages

You and device users in your organization can use stand-alone installation packages to install applications on devices manually.

A stand-alone installation package is an executable file that you can store on the Web Server or in the shared folder, send by email, or transfer to a client device by another method. On the client device, the user can run the received file locally to install an application without involving Kaspersky Security Center Linux. You can create stand-alone installation packages for Kaspersky applications and for third-party applications. To create a stand-alone installation package for a third-party application you must create a custom installation package.

Be sure that stand-alone installation package is not available for third persons.

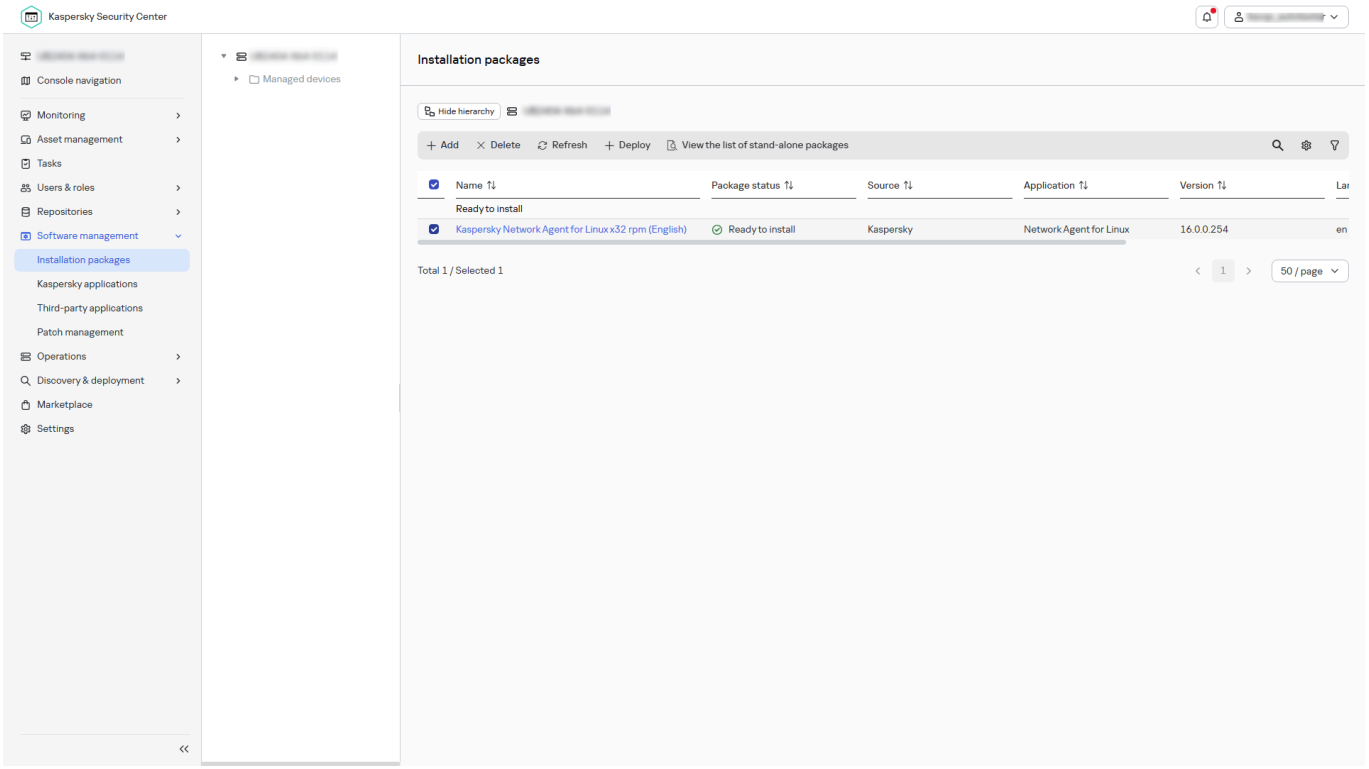
*To create a stand-alone installation package:*

1. In the main menu, go to **Software management → Installation packages**.

   A list of installation packages available on the Administration Server is displayed.

   Information about the size, file hash, and path is not available in the list of installation packages for the Network Agent stand-alone package or for any packages created on virtual Administration Servers. These stand-alone packages are generated at the time of download.

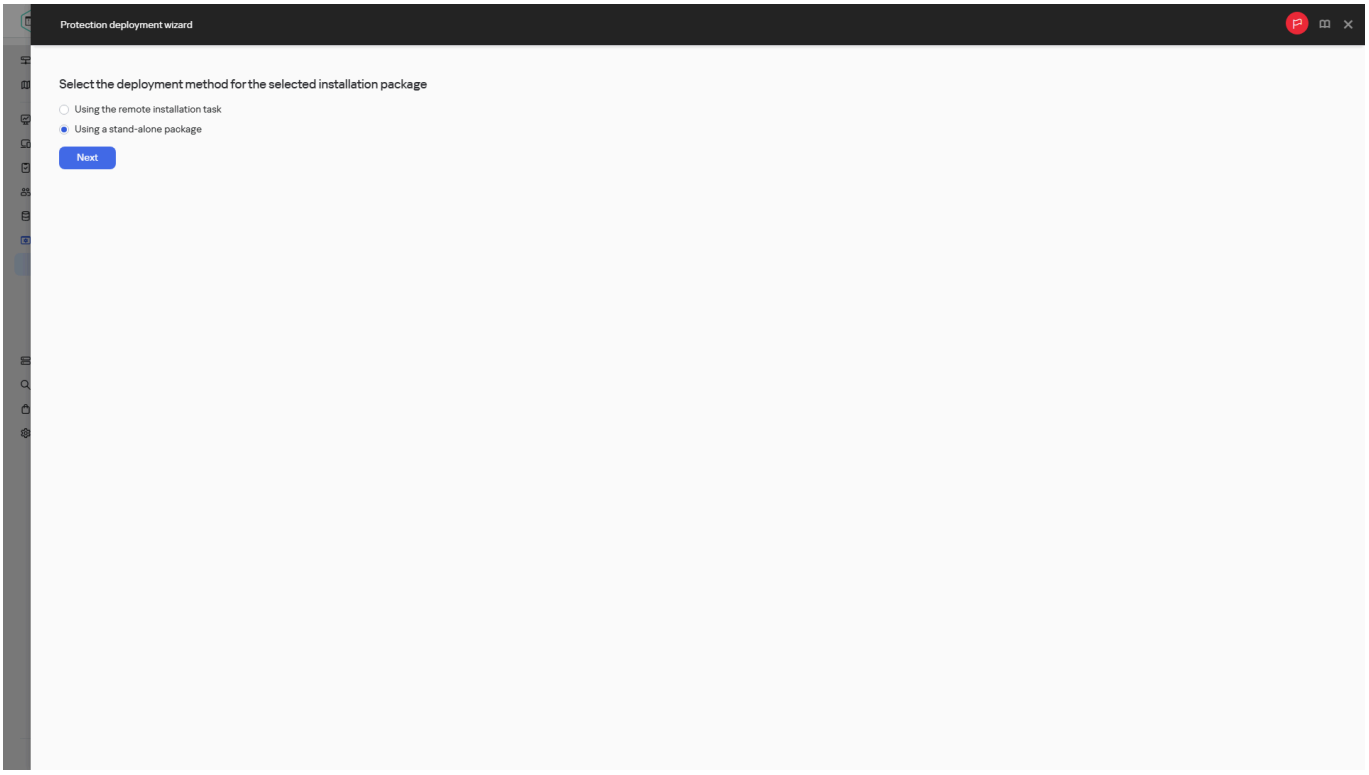
2. In the list of installation packages, select an installation package and, above the list, click the **Deploy** button.




The list of installation packages

3. Select the **Using a stand-alone package** option.

   The Stand-alone installation package creation wizard starts. Proceed through the wizard by using the **Next** button.




Selecting the deployment method for the installation package

4. Make sure that the **Install Network Agent together with this application** option is enabled if you want to install Network Agent together with the selected application.

The option is displayed depending on the application for which you create a stand-alone installation package.

By default, the option is enabled. It is recommended to enable this option if you are not sure whether Network Agent is installed on the device. If Network Agent is already installed on the device, after the stand-alone installation package with Network Agent installed Network Agent will be updated to the newer version.

If you disable this option, Network Agent will not be installed on the device and the device will be unmanaged.

If a stand-alone installation package for the selected application already exists on Administration Server, the wizard informs you about this fact. In this case, you must select one of the following actions:

- **Create stand-alone installation package**. Select this option, for example, if you want to create a stand-alone installation package for a new application version and also want to retain a stand-alone installation package that you created for a previous application version. The new stand-alone installation package is placed in another folder.
- **Use existing stand-alone installation package**. Select this option if you want to use an existing stand-alone installation package. The process of package creation will not be started.
- **Rebuild existing stand-alone installation package**. Select this option if you want to create a stand-alone installation package for the same application again. The stand-alone installation package is placed in the same folder.

5. On the **Move to list of managed devices** step, the **Do not move devices** option is selected by default. If you do not want to move the client device to any administration group after Network Agent installation, leave this option selected.

   If you want to move client device after Network Agent installation, select the **Move unassigned devices to this group** option and specify an administration group to which you want to move the client device. By default, the device is moved to the **Managed devices** group.




Selecting the administration group to move the client device

6. When the process of the stand-alone installation package creation is finished, click the **FINISH** button.

   The Stand-alone Installation Package Creation Wizard closes.

The stand-alone installation package is created and placed in the PkgInst subfolder of the Administration Server shared folder. You can view the list of stand-alone packages by clicking the **View the list of stand-alone packages** button above the list of installation packages.

# Network Agent installation package settings

*To configure a Network Agent installation package:*

1. In the main menu, go to **Software management** → **Installation packages**.

   A list of installation packages available on the Administration Server is displayed.

2. Click the name of the Network Agent installation package.

The Network Agent installation package properties window opens.

The settings of a Network Agent installation package are grouped on the following tabs:

- **General** tab

  This tab displays the following information about the installation package:

  - Installation package name
  - Name and version of the application for which the installation package has been created
  - Installation package size
  - Installation package creation date
  - Path to the installation package folder

- **Settings** tab

  This tab presents the settings required to ensure proper functioning of Network Agent immediately after it is installed.

  - **Settings** section

    **Install in default folder**

    If this option is selected, Network Agent will be installed in the <Drive>:\Program Files\Kaspersky Lab\NetworkAgent folder. If this folder does not exist, it will be created automatically.

    By default, this option is selected.

    **Install in specified folder**

    If this option is selected, Network Agent will be installed in the folder specified in the entry field.

    **Use uninstallation password**

    If this option is enabled, you can enter the uninstall password (only available for Network Agent on devices running Windows operating systems).

    By default, this option is disabled.

    **Protect Network Agent service against unauthorized removal or termination, and prevent changes to the settings**

When this option is enabled, after Network Agent is installed on a managed device, the component cannot be removed or reconfigured without required privileges. The Network Agent service cannot be stopped. This option has no effect on domain controllers.

Enable this option to protect Network Agent on workstations operated with local administrator rights.

By default, this option is disabled.

**Automatically install applicable updates and patches for components that have the Undefined status**

If this option is enabled, all downloaded updates and patches for Administration Server, Network Agent, Kaspersky Security Center Web Console, and iOS MDM Server will be installed automatically.

If this option is disabled, all downloaded updates and patches will only be installed after you change their status to *Approved*. Updates and patches with *Undefined* status will not be installed.

By default, this option is enabled.

- **Connection** section

  In this section, you can configure connection of Network Agent to the Administration Server. To establish a connection, you can use the SSL or UDP protocol. For configuring the connection, specify the following settings:

  **Administration Server address**

  Address of the device with Administration Server installed.

  **Port number**

  Port number that is used for connection.

  **SSL port**

  Port number that is used for connection over the SSL protocol.

  **Use Server certificate**

  If this option is enabled, authentication of Network Agent access to the Administration Server will use the certificate file that you can specify by clicking the **Select certificate file** button.

  If this option is disabled, the certificate file will be received from the Administration Server at the first connection of Network Agent to the address specified in the **Administration Server address** field.

  We do not recommend to disable this option, because automatic receipt of an Administration Server certificate by Network Agent upon connection to the Administration Server is considered insecure.

  By default, this option is disabled.

  **Use SSL connection**

  If this option is enabled, connection to the Administration Server is established through a secure port via SSL.

  By default, this option is disabled. We recommend that you do not disable this option so your connection remains secured.

  **Use UDP port**

  If this option is enabled, the Network Agent is connected to Administration Server through a UDP port. This allows to manage client devices and receive information about them.

  The UDP port must be open on managed devices where Network Agent is installed. Therefore, we recommend that you do not disable this option.

  By default, the option is enabled.

  **UDP port**

In this field you can specify the port to connect Administration Server to Network Agent using UDP protocol.

The default UDP port is 15000.

**Do not use proxy server**

If this option is enabled, direct connection is used to connect the device to the Administration server.

**Use proxy server**

If this option is enabled, specify the proxy server parameters:

- **Proxy server address**
- **Proxy server port**

If your proxy server requires authentication, enable the **Proxy server authentication** option and specify the **User name** and **Password** of the account under which connection to the proxy server is established. We recommend that you specify the credentials of an account that has minimum privileges required only for the proxy server authentication.

**Open Network Agent ports in Microsoft Windows Firewall**

If this option is enabled, the ports used by Network Agent are added to the Microsoft Windows Firewall exclusion list.

By default, this option is enabled.

> This option is available only for Network Agent installation packages intended for devices running Windows.

- **Advanced** section

  In this section, you can configure how to use the connection gateway.

  In the **Connection gateway** group of settings, you can configure the connection method between a device and Administration Server:

  **Use Network Agent as a connection gateway in DMZ**

  If this option is enabled, Network Agent is used as a connection gateway in the demilitarized zone (DMZ) to connect to Administration Server, communicate with it, and keep data on the Network Agent safe during data transmission.

  **Connect to Administration Server by using a connection gateway**

  If this option is enabled, connection to Administration Server is established by using a connection gateway to reduce the number of connections to the Administration Server. In this case, enter the address of the device that will act as the connection gateway in the **Connection gateway address** field.

  In the **Virtual machine** group of settings, you can configure the connection for Virtual Desktop Infrastructure (VDI) if your network includes virtual machines:

  **Enable dynamic mode for VDI**

  If this option is enabled, dynamic mode for Virtual Desktop Infrastructure (VDI) will be enabled for Network Agent installed on a virtual machine.

  By default, this option is disabled.

  **Optimize settings for VM**

If this option is enabled, the following features are disabled in the Network Agent settings:

- Retrieving information about software installed
- Retrieving information about hardware
- Retrieving information about vulnerabilities detected
- Retrieving information about updates required

By default, this option is disabled.

If you want to automatically prompt users to register as device owners after installing Network Agent on Linux devices, enable the **Allow running the user registration utility after Network Agent installation** option.

If this option is enabled, the user registration as a device owner utility will run after Network Agent installation. By default, this option is disabled.

- **Tags** section

  The **Tags** section displays a list of keywords (tags) that can be added to client devices after Network Agent installation. You can add and remove tags from the list, as well as rename them.

  If the check box is selected next to a tag, this tag is automatically added to managed devices during Network Agent installation.

  If the check box is cleared next to a tag, the tag will not automatically be added to managed devices during Network Agent installation. You can manually add this tag to devices.

  When removing a tag from the list, it is automatically removed from all devices to which it was added.

  > Automatic tagging rules are not applicable to Network Agent installation packages intended for devices running Linux and macOS.

- **Stand-alone packages** tab

  On this tab, you can do the following:

  - View the list of available stand-alone installation packages.
  - Publish a stand-alone installation package on the Web Server by clicking the **Publish** button. Published stand-alone installation package is available for downloading for users whom you sent the link to the stand-alone installation package.
  - Cancel publication of a stand-alone installation package on the Web Server by clicking the **Unpublish** button. Unpublished stand-alone installation package is available for downloading only for you and other administrators.
  - Download a stand-alone installation package to your device by clicking the **Download** button.
  - Send email with the link to a stand-alone installation package by clicking the **Send by email** button.
  - Remove a stand-alone installation package by clicking the **Remove** button.

- **Revision history** tab

  On this tab, you can view the history of the installation package revisions. You can compare revisions, view revisions, save revisions to a file, and add and edit revision descriptions.

# Running stand-alone packages created by Kaspersky Security Center Linux

The above-described methods of initial deployment of Network Agent and other applications cannot always be implemented because it is not possible to meet all of the applicable conditions. In such cases, you can create a common executable file called a *stand-alone installation package* through Kaspersky Security Center Linux, using installation packages with the relevant installation settings that have been prepared by the administrator. A stand-alone installation package can be published either on an internal Web Server (included in Kaspersky Security Center Linux) if this is deemed reasonable (outside access to that Web Server has been configured for target device users), or on an exclusively deployed Web Server included in Kaspersky Security Center Web Console. You can also copy stand-alone packages to another Web Server.

You can use Kaspersky Security Center Linux to send selected users an email message containing a link to the stand-alone package file on the currently used Web Server, prompting them to run the file (either in interactive mode, or with the "-s" key for silent installation). You can attach the stand-alone installation package to an email message and then send it to the users of devices that have no access to the Web Server. The administrator can also copy the stand-alone package to a removable drive, deliver it to a relevant device, and then run it later.

You can create a stand-alone package from a Network Agent package, a package of another application (for example, the security application), or both. If the stand-alone package has been created from Network Agent and another application, installation starts with Network Agent.

When creating a stand-alone package with Network Agent, you can specify the administration group to which new devices (those that have not been allocated to any of the administration groups) will be automatically moved when Network Agent installation completes on them.

Stand-alone packages can run in interactive mode (by default), displaying the result for installation of applications they contain, or they can run in silent mode (when run with the key "-s"). Silent mode can be used for installation from scripts, for example, from scripts configured to run after an operating system image is deployed. The result of installation in silent mode is determined by the return code of the process.

# Installing applications by using stand-alone packages

Kaspersky Security Center lets you create stand-alone installation packages for applications. A stand-alone installation package is an executable file that can be located on the Web Server, sent by email, or transferred to a client device by another method. The received file can be run locally on the client device to install an application without involving Kaspersky Security Center.

*To install an application by using a stand-alone installation package:*

1. In the main menu, go to **Software management** → **Installation packages**.
2. Select the check box next to the installation package of the required application, and then click the **Deploy** button.
3. In the window that opens, select **Using a stand-alone package**, and then click the **Next** button.

   The Stand-alone installation package creation wizard starts. Proceed through the wizard by using the **Next** button.
4. Select the **Create stand-alone installation package** option.

5. Specify whether devices must be moved to an administration group after Network Agent installation.

6. At the final step of the wizard, select a method for transferring the stand-alone installation package to the client device, and then click the **Finish** button to finish the wizard.

7. Transfer the stand-alone installation package to the client device.

8. Run the stand-alone installation package on the client device.

The application is now installed on the client device with the settings specified in the stand-alone package.

When you create a stand-alone installation package, it is automatically published on Web Server. The link for downloading the stand-alone package is displayed in the list of created stand-alone installation packages. If necessary, you can cancel publication of the selected stand-alone package and republish it on the Web Server. By default, port 8060 is used for downloading stand-alone installation packages.

# Suitability of databases updating in an installation package of a security application

Before starting the protection deployment, you must keep in mind the possibility of updating anti-virus databases (including modules of automatic patches) shipped together with the distribution package of the security application. It is useful to update the databases in the installation package of the application before starting the deployment (for example, by using the corresponding command in the context menu of a selected installation package). This will reduce the number of restarts required for completion of protection deployment on target devices.

# Changing the limit on the size of custom installation package data

The total size of data unpacked during creation of a custom installation package is limited. The default limit is 1 GB.

If you attempt to upload an archive file that contains data exceeding the current limit, an error message is displayed. You might have to increase this limit value when creating installation packages from large distribution packages.

*To change the limit value for the custom installation package size:*

1. On the Administration Server device, run the command prompt under the account that was used to install Administration Server.

2. Change your current directory to the Kaspersky Security Center Linux installation folder (usually, /opt/kaspersky/ksc64/sbin).

3. Depending on the type of Administration server installation, enter one of the following commands under the root account:

   - Normal local installation:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes>
     ```

   - Installation on the Kaspersky Security Center Linux failover cluster:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes> --stp
     klfoc
     ```

Where <number of bytes> is a number of bytes in hexadecimal or decimal format.

For example, if the required limit is 2 GB, you can specify the decimal value 2147483648 or the hexadecimal value 0x80000000. In this case, for a local installation of Administration Server, you can use the following command:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
```

The limit on the size of custom installation package data is changed.

# Distributing installation packages to secondary Administration Servers

Kaspersky Security Center Linux allows you to create installation packages for Kaspersky applications and for third-party applications, as well as distribute installation packages to client devices and install applications from the packages. To optimize the load on the primary Administration Server, you can distribute installation packages to secondary Administration Servers. After that, the secondary Servers transmit the packages to client devices, and then you can perform the remote installation of the applications on your client devices.

*To distribute installation packages to secondary Administration Servers:*

1. Make sure that the secondary Administration Servers are connected to the primary Administration Server.
2. In the main menu, go to **Tasks**.

   The list of tasks is displayed.
3. Click **Add**.

   The New task wizard starts. Follow the steps of the wizard.
4. On the **New task settings** page, from the **Application** drop-down list, select **Kaspersky Security Center**. Then, from the **Task type** drop-down list, select **Distribute installation package**, and then specify the task name.
5. On the **Task scope** page, select the devices to which the task is assigned in one of the following ways:

   - If you want to create a task for all secondary Administration Servers in a specific administration group, select this group, and then create a group task for it.
   - If you want to create a task for specific secondary Administration Servers, select these Servers, and then create a task for them.
6. On the **Distributed installation packages** page, select the installation packages that are to be copied to the secondary Administration Servers.
7. Specify an account to run the *Distribute installation package* task under this account. You can use your account and keep the **Default account** option enabled. Alternatively, you can specify that the task should be run under another account that has the necessary access rights. To do this, select the **Specify account** option, and then enter the credentials of that account.
8. On the **Finish task creation** page, you can enable the **Open task details when creation is complete** option to open the task properties window, and then modify the default task settings. Otherwise, you can configure the task settings later, at any time.

9. Click the **Finish** button.

   The task created for distributing installation packages to the secondary Administration Servers is displayed in the task list.

10. Run the task manually or wait for it to launch according to the schedule that you specified in the task settings.

    After the task is completed, the selected installation packages are copied to the specified secondary Administration Servers.

# Viewing the list of stand-alone installation packages

You can view the list of stand-alone installation packages and properties of each stand-alone installation package.

*To view the list of stand-alone installation packages for all installation packages:*

Above the list, click the **View the list of stand-alone packages** button.

In the list of stand-alone installation packages, their properties are displayed as follows:

- **Package name**. Stand-alone installation package name that is automatically formed as the application name included in the package and the application version.
- **Application name**. Application name included in the stand-alone installation package.
- **Application version**.
- **Network Agent installation package name**. The property is displayed only if Network Agent is included in the stand-alone installation package.
- **Network Agent version**. The property is displayed only if Network Agent is included in the stand-alone installation package.
- **Size**. File size in MB.
- **Group**. Name of the group to which the client device is moved after Network Agent installation.
- **Created**. Date and time of the stand-alone installation package creation.
- **Modified**. Date and time of the stand-alone installation package modification.
- **Path**. Full path to the folder where the stand-alone installation package is located.
- **Web address**. Web address of the stand-alone installation package location.
- **File hash**. The property is used to certify that the stand-alone installation package was not changed by third-party persons and a user has the same file you have created and transferred to the user.

Information about the size, file hash, and path is not available in the list of installation packages for the Network Agent stand-alone package or for any packages created on virtual Administration Servers. These stand-alone packages are generated at the time of download.

*To view the list of stand-alone installation packages for specific installation package:*

Select the installation package in the list and, above the list, click the **View the list of stand-alone packages** button.

In the list of stand-alone installation packages, you can do the following:

- Publish a stand-alone installation package on the Web Server by clicking the **Publish** button. Published stand-alone installation package is available for downloading for users whom you sent the link to the stand-alone installation package.
- Cancel publication of a stand-alone installation package on the Web Server by clicking the **Unpublish** button. Unpublished stand-alone installation package is available for downloading only for you and other administrators.
- Download a stand-alone installation package to your device by clicking the **Download** button.
- Send email with the link to a stand-alone installation package by clicking the **Send by email** button.
- Remove a stand-alone installation package by clicking the **Remove** button.

# Installing Network Agent for Linux

To manage devices in an organization, you have to install Network Agent on each of them. Deployment of distributed Kaspersky Security Center Linux on corporate devices normally begins with installation of Network Agent on them.

There are the following methods to initially install Network Agent on the Linux managed device:

- By connecting to the managed device through SSH and running the remote installation task.
- By running the package installation on the managed device.

After Network Agent is installed on a device, you can perform the remote installation of Kaspersky applications on that device through this Network Agent. The distribution package of an application to be installed is transferred over communication channels between Network Agents and Administration Server, along with the installation settings defined by the administrator. To transfer the distribution package, you can use relay distribution nodes, that is, distribution points, multicast delivery, etc.

When selecting a method and a strategy for deployment of applications on a managed network, you must consider a number of factors (partial list):

- Organization's network configuration.
- Total number of devices.
- Presence of devices on the organization's network, which are not members of any domain, and presence of uniform accounts with administrator rights on those devices.
- Capacity of the channel between the Administration Server and devices.

- Type of communication between Administration Server and remote subnets and capacity of network channels in those subnets.
- Security settings applied on remote devices at the start of deployment. These parameters allow to establish the remote connection to the managed device and start the installation.

# Preparing a Linux device for installation of Network Agent

Prior to the installation of Network Agent on a Linux device, you must perform preparation steps that are required for any Linux device.

*To prepare a device running Linux for remote installation of Network Agent:*

1. Make sure that the device on which you want to install Network Agent for Linux is running one of the supported Linux distributions.
2. If you want to install Network Agent on AltOS in the closed software environment mode, disable the closed software environment mode until the installation is finished.
3. Download the Network Agent installation package by using the Web Console interface or from the Kaspersky website.

   If you need to install Network Agent on a device running a Linux operating system with glibc 2.5, you must download the *Kaspersky Network Agent for Linux Legacy* installation package by using the Web Console interface or from the Kaspersky website.
4. Make sure that the following software is installed on the target Linux device:
   - Sudo (for Ubuntu 10.04, Sudo version is 1.7.2p1 or later)
   - Perl language interpreter version 5.10 or later
   - ps utility
5. Test the device configuration:
   a. Check whether you can connect to the device through an SSH client (such as PuTTY).

      If you cannot connect to the device, open the `/etc/ssh/sshd_config` file and make sure that the following settings have the respective values listed below:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      Do not modify the /etc/ssh/sshd_config file if you can connect to the device with no issues; otherwise, you may encounter SSH authentication failure when running a remote installation task.

      Save the file (if necessary) and restart the SSH service by using the `sudo service ssh restart` command.

   b. Ensure that port TCP 22 is open and accessible on a Linux-based unassigned device.

      TCP port 22 must be available for successful installation of Network Agent for Linux.

   c. Disable the sudo password for the user account under which the device is to be connected.

d. Use the `visudo` command in sudo to open the sudoers configuration file.

In the file you have opened, add the following line to the end of the file: `<username> ALL = (ALL) NOPASSWD: ALL`. In this case, `<username>` is the user account which is to be used for the device connection using SSH. If you are using the Astra Linux operating system, in the /etc/sudoers file, add the last line with the following text: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. Save the sudoers file and then close it.

f. Connect to the device again through SSH and make sure that the Sudo service does not prompt you to enter a password; you can do this using the `sudo whoami` command.

6. If you want to install Network Agent remotely on devices running operating system with the systemd initialization system, open the `/etc/systemd/logind.conf` file, and then do one of the following:

- Specify `no` as a value for the `KillUserProcesses` setting: `KillUserProcesses=no`.
- For the `KillExcludeUsers` setting, type the user name of the account under which the remote installation is to be performed, for example, `KillExcludeUsers=root`.

**Astra Linux target device**

If the target device is running Astra Linux, add `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` string in the `/home/<username>/.bashrc` file, where `<username>` is the user account which is to be used for the device connection using SSH.

**OSnova target device**

If the target device is running OSnova, do the following:

a. Open the `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` file, and then comment out the `#KillUserProcess=yes` line.

b. Open the `/usr/lib/NESS/pam-user-session` file, and then comment out the `#loginctl terminate-session "$XDG_SESSION_ID"` line.

To apply the changed setting, restart the Linux device or execute the following command:

```
sudo systemctl restart systemd-logind.service
```

7. If you want to install Network Agent on devices with the SUSE Linux Enterprise Server 15 operating system, install the insserv-compat package first to configure Network Agent.

8. If you want to install Network Agent on devices that have the Astra Linux operating system running in the closed software environment mode, perform additional steps to prepare Astra Linux devices.

9. If you want to install Network Agent on devices running Ubuntu Server or Ubuntu Desktop version 10.04, perform additional steps to prepare these devices.

10. If you want to install Network Agent on a device running a Linux operating system with glibc 2.5, perform additional steps to prepare the target devices.

11. If you're installing Network Agent on AltOS in the closed software environment mode, re-enable the closed software environment mode.

12. If you want to install Network Agent on devices that use the operating system RED OS 7.3.4 or later or MSVSPHERE 9.2 or later, install the libxcrypt-compat package for the correct function of Network Agent.

The Linux device is ready for installation of Network Agent. You can install Network Agent remotely, in interactive mode, or in silent mode.

# Preparing a device running SUSE Linux Enterprise Server 15 for installation of Network Agent

Prior to the installation of Network Agent on a device running SUSE Linux Enterprise Server 15, you must perform two preparation procedures—the one in the instructions below and general preparation steps for any Linux device.

*To install Network Agent on a device with the SUSE Linux Enterprise Server 15 operating system:*

Before the Network Agent installation, run the following command:

```
sudo zypper install insserv-compat
```

This enables you to install the insserv-compat package and configure Network Agent properly.

> Run the `rpm -q insserv-compat` command to check whether the package is already installed.

If your network includes a lot of devices running SUSE Linux Enterprise Server 15, you can use the special software for configuring and managing the company infrastructure. By using this software, you can automatically install the insserv-compat package on all necessary devices at once. For example, you can use Puppet, Ansible, Chef, you can make your own script—use any method that is convenient for you.

If the device does not have the GPG signing keys for SUSE Linux Enterprise, you may encounter the following warning: `Package header is not signed!` Select the `i` option to ignore the warning.

After preparing the Linux device, you can install Network Agent remotely, in interactive mode, or in silent mode.

# Preparing a device running Astra Linux in the closed software environment mode for installation of Network Agent

Prior to the installation of Network Agent on a device running Astra Linux in the closed software environment mode, you must perform two preparation procedures—the one in the instructions below and general preparation steps for any Linux device.

> Run the commands provided in this instruction under an account with root privileges.

*To prepare a device running Astra Linux in the closed software environment mode for installation of Network Agent:*

1. Open the `/etc/digsig/digsig_initramfs.conf` file, and then specify the following setting:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. In the command line, run the following command to install the compatibility package:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Create a directory for the application key:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Place the application key /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg in the directory created in the previous step:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   If the Kaspersky Security Center Linux distribution kit does not include the kaspersky_astra_pub_key.gpg application key, you can download it by clicking the link: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Update the RAM disks:

   ```
   update-initramfs -u -k all
   ```

   Reboot the system.

The Linux device is ready for installation of Network Agent. You can install Network Agent remotely, in interactive mode, or in silent mode.

# Preparing to install Network Agent on a Linux operating system with glibc 2.5 (legacy OS)

Prior to the installation of Network Agent on a device running a Linux operating system with glibc 2.5 (legacy OS), you must perform two preparation procedures—general preparation steps for any Linux device and the procedure described in this article.

We recommend that you use local installation to install Network Agent on a Linux operating system with glibc 2.5 (legacy OS). If you need to use a remote installation task for this scenario, you must perform additional steps described in the instruction below.

Run the commands provided in this procedure under an account with root privileges.

We recommend that you use local installation to install Network Agent on a Linux operating system with glibc 2.5 (legacy OS). If you need to use a remote installation task for this scenario, you must perform additional steps described in the instruction below.

1. On the device running a Linux operating system with glibc 2.5, perform the preparation steps common for any Linux device.

2. In the `/etc/sudoers` file, remove the line `Defaults requiretty`.

3. Disable the allowlist of valid encryption algorithms for SSH connections to be able to install Network Agent on the device running a Linux operating system with glibc 2.5.

   To do this, on the device with Administration Server installed, or on a device acting as a distribution point whose scope includes the target device, run the following command in the command line:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

The Linux device is ready for remote installation of Network Agent.

Disabling the allowlist of valid encryption algorithms may affect the security of the SSH connection. We strongly recommend that you re-enable the allowlist of valid encryption algorithms immediately after installing Network Agent. To re-enable the allowlist of valid encryption algorithms, run the following command:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

Once you installed the Network Agent and then re-enabled the allowlist of valid encryption algorithms, the device running a Linux operating system with glibc 2.5 (legacy OS) is now managed by the Administration Server.

# Preparing to install Network Agent on a Linux operating system with OpenSSH version 6.4 (legacy OS)

Prior to the installation of Network Agent on a device that uses OpenSSH version 6.4 or earlier (legacy OS), you must perform two preparation procedures—general preparation steps for any Linux device and the procedure described in this article.

We recommend that you use local installation to install Network Agent on a Linux operating system with glibc 2.5 (legacy OS). If you need to use a remote installation task for this scenario, you must perform additional steps described in the instruction below.

> Run the commands provided in this instruction under an account with root privileges.

*To prepare a device that uses OpenSSH version 6.4 or earlier for installation of Network Agent:*

1. On the device that uses OpenSSH version 6.4 or earlier, perform the preparation steps common for any Linux device.

2. Disable the allowlist of valid encryption algorithms for SSH connections to be able to install Network Agent on the device that uses OpenSSH version 6.4 or earlier.

   To do this, on the device with Administration Server installed, or on a device acting as a distribution point whose scope includes the target device, run the following command in the command line:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

The Linux device is ready for remote installation of Network Agent.

Disabling the allowlist of valid encryption algorithms may affect the security of the SSH connection. We strongly recommend that you re-enable the allowlist of valid encryption algorithms immediately after installing Network Agent. To re-enable the allowlist of valid encryption algorithms, run the following command:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

Once you installed the Network Agent and then re-enabled the allowlist of valid encryption algorithms, the device running a Linux operating system with glibc 2.5 (legacy OS) is now managed by the Administration Server.

# Installing Network Agent on a Linux device remotely

Before installing Network Agent on a Linux-based device, you must complete the general preparatory steps that are required to all Linux-based devices.

After completing the general steps, you can follow the additional instructions specific to your operating system:

- Preparing a device running SUSE Linux Enterprise Server 15
- Preparing a device running Astra Linux in the closed software environment mode
- Preparing a device running Ubuntu Server/Desktop version 10.04 and 16.04
- Preparing a device running a Linux operating system with glibc 2.5

*To install Network Agent on Linux devices remotely:*

1. Download and create an installation package:

   a. Before installing the package on the device, make sure that it already has all the dependencies (programs and libraries) installed for this package.

   You can view the dependencies for each package on your own, using utilities that are specific for the Linux distribution on which the package is to be installed. For more details about utilities, refer to your operating system documentation.

   b. To create a remote installation package, use the following files:

   - klnagent.kpd
   - akinstall.sh
   - .deb or .rpm package of Network Agent

2. Create a remote installation task with the following settings:

   - On the **Settings** page of the New task wizard, select the **Using operating system resources through Administration Server** check box. Clear all other check boxes.
   - On the **Selecting an account to run the task** page specify the settings of the user account that is used for device connection through SSH.

3. Run the remote installation task. Use the option for the `su` command to preserve the environment: `-m, -p, --preserve-environment`.

# Installing Network Agent for Linux in silent mode (with an answer file)

You can install Network Agent on Linux devices by using an answer file—a text file that contains a custom set of installation parameters: variables and their respective values. Using this answer file allows you to run an installation in silent mode, that is, without user participation.

Before installing Network Agent on a Linux-based device, you must complete the general preparatory steps that are required to all Linux-based devices.

After completing the general steps, you can follow the additional instructions specific to your operating system:

- Preparing a device running SUSE Linux Enterprise Server 15
- Preparing a device running Astra Linux in the closed software environment mode
- Preparing a device running Ubuntu Server/Desktop version 10.04 and 16.04
- Preparing a device running a Linux operating system with glibc 2.5

*To perform installation of Network Agent for Linux in silent mode:*

1. Read the End User License Agreement. Follow the steps below only if you understand and accept the terms of the End User License Agreement.

2. Create the answer file (in TXT format). Add to the answer file a list of variables in the VARIABLE_NAME=variable_value format, each variable on a separate line.

   For correct usage of the answer file, you must include in it a minimum set of the three required variables:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   You can also add any optional variables to use more specific parameters of your remote installation. The following table lists all of the variables that can be included in the answer file:

   **Variables of the answer file used as parameters of Network Agent for Linux installation in silent mode**

   Variables of the answer file used as parameters of Network Agent for Linux installation in silent mode

| Variable name | Required | Description | Possible values |
|---|---|---|---|
| KLNAGENT_SERVER | Yes | Contains the Administration Server name presented as fully qualified domain name (FQDN) or IP address. | DNS name or IP address. |
| KLNAGENT_AUTOINSTALL | Yes | Defines whether silent installation mode is enabled. | 1—Silent mode is enabled; the user is not prompted for any actions during installation.<br><br>Other—Silent mode is disabled; the user may be prompted for actions during installation. |
| EULA_ACCEPTED | Yes | Defines whether the user accepts the End User License Agreement (EULA) of Network Agent; when missing, can be interpreted as non-acceptance of the EULA. | 1—I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement.<br><br>Other or not specified—I do not accept the terms of the License Agreement (installation is not performed). |
| KLNAGENT_PROXY_USE | No | Defines whether connection with the Administration Server will use proxy settings. The default value is 0. | 1—Proxy settings are used.<br><br>Other—Proxy settings are not used. |

| | | | |
|---|---|---|---|
| KLNAGENT_PROXY_ADDR | No | Defines the address of the proxy server used for connection with the Administration Server. | DNS name or IP address. |
| KLNAGENT_PROXY_LOGIN | No | Defines the user name used for login to the proxy server. | Any existing user name. |
| KLNAGENT_PROXY_PASSWORD | No | Defines the user password used for login to the proxy server. | Any set of alphanumeric characters allowed by the password format in the operating system. |
| KLNAGENT_VM_VDI | No | Defines whether Network Agent is installed on an image for creation of dynamic virtual machines. | 1—Network Agent is installed on an image, which is subsequently used for creation of dynamic virtual machines.<br><br>Other—No image is used during installation. |
| KLNAGENT_VM_OPTIMIZE | No | Defines whether the Network Agent settings are optimal for hypervisor. | 1—The default local settings of Network Agent are modified so that they allow optimized usage on hypervisor. |
| KLNAGENT_TAGS | No | Lists the tags assigned to the Network Agent instance. | One or multiple tag names separated with semicolon. |
| KLNAGENT_UDP_PORT | No | Defines the UDP port used by Network Agent. The default value is 15000. | Any existing port number. |
| KLNAGENT_PORT | No | Defines the non-TLS port used by Network Agent. The default value is 14000. | Any existing port number. |
| KLNAGENT_SSLPORT | No | Defines the TLS port used by Network Agent. The default value is 13000. | Any existing port number. |
| KLNAGENT_USESSL | No | Defines whether Transport Layer Security (TLS) is used for connection. | 1 (default)—TLS is used.<br><br>Other—TLS is not used. |
| KLNAGENT_GW_MODE | No | Defines whether connection gateway is used. | 1 (default)—The current settings are not modified (at the first call, no connection gateway is specified).<br><br>2—No connection gateway is used.<br><br>3—Connection gateway is used. KLNAGENT_GW_ADDRESS is required.<br><br>4—The Network Agent instance is used as connection gateway in demilitarized zone (DMZ). Server certificate is required. |
| KLNAGENT_GW_ADDRESS | No | Defines the address of the connection gateway. The value is applicable only if KLNAGENT_GW_MODE=3. | DNS name or IP address. |
| KLNAGENT_DEVICEOWNER_REGISTRATION_START | No | Allows to run the user registration as a device owner utility after Network Agent installation. If turned off, then the registration as a device owner is not available to a user. | 1—The user registration as a device owner utility will run after Network Agent installation.<br><br>Other—Turned off. |
| PTCH_ALLOW_APPLY_NONAPROVED_PATCHES | No | Defines whether to install the downloaded updates automatically for Network Agent with the *Undefined* status. | true (default)—Updates are installed automatically.<br><br>false—Updates are not installed automatically. |

3. Run the Network Agent installation. The KLAUTOANSWERS environment variable, which specifies the path to the answer file, is passed to the installation command. Run one of the following command:

   - To install Network Agent from an RPM package to a 32-bit operating system, execute the following command:
     `sudo KLAUTOANSWERS=<path to answer file> yum install ./klnagent-<build number>.i386.rpm`

   - To install Network Agent from an RPM package to a 64-bit operating system, execute the following command:
     `sudo KLAUTOANSWERS=<path to answer file> yum install ./klnagent64-<build number>.x86_64.rpm`

   - To install Network Agent from an RPM package on a 64-bit operating system for the Arm architecture, execute the following command:
     `sudo KLAUTOANSWERS=<path to answer file> yum install ./klnagent64-<build number>.aarch64.rpm`

   - To install Network Agent from a DEB package to a 32-bit operating system, execute the following command:
     `sudo KLAUTOANSWERS=<path to answer file> apt install ./klnagent_<build number>_i386.deb`

   - To install Network Agent from a DEB package to a 64-bit operating system, execute the following command:
     `sudo KLAUTOANSWERS=<path to answer file> apt install ./klnagent64_<build number>_amd64.deb`

   - To install Network Agent from a DEB package on a 64-bit operating system for the Arm architecture, execute the following command:
     `sudo KLAUTOANSWERS=<path to answer file> apt install ./klnagent64_<build number>_arm64.deb`

   Depending on the operating system configuration, you can also use the rpm, dpkg, or dnf package managers to install Network Agent.

Installation of Network Agent for Linux starts in silent mode; the user is not prompted for any actions during the process.

# Installing Network Agent for Linux in interactive mode

This article describes how to install Network Agent on Linux devices in the interactive mode, by specifying installation parameters step by step. Alternatively, you can use an answer file—a text file that contains a custom set of installation parameters: variables and their respective values. Using this answer file allows you to run an installation in silent mode, that is, without user participation.

Before installing Network Agent on a Linux-based device, you must complete the general preparatory steps that are required to all Linux-based devices.

After completing the general steps, you can follow the additional instructions specific to your operating system:

- Preparing a device running SUSE Linux Enterprise Server 15
- Preparing a device running Astra Linux in the closed software environment mode

- Preparing a device running Ubuntu Server/Desktop version 10.04 and 16.04
- Preparing a device running a Linux operating system with glibc 2.5

*To install Network Agent in interactive mode:*

1. Run the Network Agent installation. Depending on your Linux distribution, run one of the following commands:
   - To install Network Agent from an RPM package to a 32-bit operating system:
     `# yum -i klnagent-<build number>.i386.rpm`
   - To install Network Agent from an RPM package to a 64-bit operating system:
     `# yum -i klnagent64-<build number>.x86_64.rpm`
   - To install Network Agent from an RPM package on a 64-bit operating system for the Arm architecture:
     `# yum -i klnagent64-<build number>.aarch64.rpm`
   - To install Network Agent from a DEB package to a 32-bit operating system:
     `# apt install ./klnagent_<build number>_i386.deb`
   - To install Network Agent from a DEB package to a 64-bit operating system:
     `# apt install ./klnagent64_<build number>_amd64.deb`
   - To install Network Agent from a DEB package on a 64-bit operating system for the Arm architecture:
     `# apt install ./klnagent64_<build number>_arm64.deb`
2. Run the Network Agent configuration:
   `# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl`
3. Read the End User License Agreement. The text is displayed in the command line window. Press the space bar to view the next text segment. Then, when prompted, enter one the following values:
   - Enter `y` if you understand and accept the terms of the EULA.
   - Enter `n` if you do not accept the terms of the EULA. To use Network Agent, you must accept the terms of the EULA.
   - Enter `r` to show the EULA again.
4. Enter the Administration Server DNS name or IP address.
5. Enter the Administration Server port number. The default port number is 14000.
6. Enter the Administration Server SSL port number. The default port number is 13000.
7. Enter `y` if you want to use SSL encryption for traffic between Network Agent and Administration Server. Otherwise, enter `n`.
8. Select one of the following options to configure Network Agent:
   - `[1]` – `Keep current connection gateway settings`.
     During initial installation, a connection gateway is not configured. When upgrading, previously specified connection gateway settings are used.

- `[2] – Do not use connection gateway.`

  Your device will not connect to Administration Server through a connection gateway.

- `[3] –Connect to server using connection gateway.`

  Your device will connect to Administration Server through a connection gateway.

- `[4] – Use as connection gateway.`

  Your device will act as a connection gateway.

Network Agent is installed on a Linux device.

# Support of file system rollback for devices with Network Agent

Kaspersky Security Center Linux is a distributed application. Rolling back the file system to a previous state on a device with Network Agent installed will lead to data desynchronization and improper functioning of Kaspersky Security Center Linux.

The file system (or a part of it) can be rolled back in the following cases:

- When copying an image of the hard drive.
- When restoring a state of the virtual machine by means of the virtual infrastructure.
- When restoring data from a backup copy or a recovery point.

Scenarios under which third-party software on devices with Network Agent installed affects the /var/opt/kaspersky/klnagent directory are only critical scenarios for Kaspersky Security Center Linux. Therefore, you must always exclude this folder from the recovery procedure, if possible.

Because the workplace rules of some organizations provide for rollbacks of the file system on devices, support for the file system rollback on devices with Network Agent installed has been added to Kaspersky Security Center Linux, starting with version 10 Maintenance Release 1 (Administration Server and Network Agents must be of version 10 Maintenance Release 1 or later). When detected, those devices are automatically reconnected to the Administration Server with full data cleansing and full synchronization.

By default, support of file system rollback detection is enabled in Kaspersky Security Center Linux.

As much as possible, avoid rolling back the /var/opt/kaspersky/klnagent directory on devices with Network Agent installed, because full resynchronization of data requires a large amount of resources.

A rollback of the system state is absolutely not allowed on a device with Administration Server installed. Nor is a rollback of the database used by Administration Server.

You can restore a state of Administration Server from a backup copy only with the standard klbackup utility.

# Installing Network Agent for Windows

You can also install Network Agent on Windows-based devices of an organization to manage them by using Administration Server.

In Microsoft Windows XP, Network Agent might not perform the following operations correctly: downloading updates directly from Kaspersky servers (as a distribution point) and functioning as a KSN proxy server (as a distribution point); and detecting third-party vulnerabilities (if Vulnerability and patch management is used).

Before installing the Network Agent on a device running Microsoft Windows on Arm, ensure that no Network Agent for Microsoft Windows x86-64 is already installed. Otherwise, the installation will fail.

There are the following methods to initially install Network Agent on the Windows managed device:

- By running the remote installation task through the Windows distribution point.

  Before performing a remote installation on an unassigned Windows device, a Windows-based distribution point automatically checks UDP port 137 to determine the operating system type of the target device. If UDP port 137 is unavailable, the distribution point attempts to connect to TCP port 445 on the target device, which is required to perform the installation.

- By using the Windows Installer package (MSI) for Network Agent, with third-party tools for remote installation of applications.

- By running the application installer on the managed device.

- By sending device users links to stand-alone packages generated by Kaspersky Security Center Linux. Stand-alone packages are executable modules that contain the distribution packages of selected applications with their settings defined.

# Installing Network Agent for Windows in interactive mode

*To install Network Agent on a device locally:*

1. On the device, run the ksc_<version number>.<build number>_full_<localization language>.exe file from the distribution package downloaded from the internet.

   A window opens prompting you to select Kaspersky applications to install.

2. In the application selection window, click the **Install only Kaspersky Security Center Network Agent** link to start the Network Agent setup wizard. Follow the steps of the wizard.

   While the installation wizard is running, you can specify the advanced settings of Network Agent (see below).

3. If you want to use your device as the connection gateway for a specific administration group, in the **Connection gateway** window of the setup wizard select **Use Network Agent as a connection gateway in DMZ**.

4. To configure Network Agent during installation on a virtual machine:

    a. If you plan to create dynamic virtual machines from the virtual machine image, enable dynamic mode of Network Agent for Virtual Desktop Infrastructure (VDI). To do this, in the **Advanced Settings** window of the setup wizard, select the **Enable dynamic mode for VDI** option.

    Skip this step if you do not plan to create dynamic virtual machines from the virtual machine image.

    b. Optimize the Network Agent operation for VDI. To do this, in the **Advanced Settings** window of the setup wizard, select the **Optimize settings for VM** option.

    Scanning of executable files for vulnerabilities at the device startup will be disabled. Also, this disables the sending of information about the following objects to Administration Server:

    - Hardware registry
    - Applications installed on the device
    - Microsoft Windows updates that must be installed on the local client device
    - Software vulnerabilities detected on the local client device

    Furthermore, you will be able to enable the sending of this information in the Network Agent properties or in the Network Agent policy settings.

When the setup wizard finishes, Network Agent will be installed on the device.

You can view the properties of the Network Agent service; you can also start, stop, and monitor Network Agent activity by means of standard Microsoft Windows tools: Computer Management\Services.

# Installing Network Agent for Windows in silent mode

Network Agent can be installed in silent mode, that is, without the interactive input of installation parameters. Silent installation uses a Windows Installer package (MSI) for Network Agent. The MSI file is located in the Kaspersky Security Center Linux distribution package, in the Packages\NetAgent\exec folder.

> Installation of Network Agent from the MSI package is possible only in silent mode, interactive installation from the MSI package is not supported.

*To install Network Agent on a local device in silent mode:*

1. Read the End User License Agreement. Use the command below only if you understand and accept the terms of the End User License Agreement.

2. Run the command

    ```
    msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
    ```

    where `setup_parameters` is a list of parameters and their respective values, separated by a space (`PROP1=PROP1VAL PROP2=PROP2VAL`).

    In the list of parameters, you must include `EULA=1`. Otherwise Network Agent will not be installed.

If you are using the standard connection settings for Kaspersky Security Center, and Network Agent on remote devices, run the command:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` is the key for writing logs. The log is created during the installation of Network Agent and saved at C:\windows\temp\nag_inst.log.

In addition to nag_inst.log, the application creates the $klssinstlib.log file, which contains the installation log. This file is stored in the %windir%\temp or %temp% folder. For troubleshooting purposes, you or a Kaspersky Technical Support specialist may need both log files—nag_inst.log and $klssinstlib.log.

If you need to additionally specify the port for connection to the Administration Server run the command:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

The parameter `SERVERPORT` corresponds to the number of port for connection to Administration Server.

The names and possible values for parameters that can be used when installing Network Agent in silent mode are listed in the Network Agent installation parameters section.

If you want to upgrade Network Agent using Windows Installer, run the following command:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

# Deployment by capturing and copying the image of a device

If you need to install Network Agent on devices on which an operating system and other software also must be installed (or reinstalled), you can use the mechanism of capturing and copying the image of that device.

*To perform deployment by capturing and copying a hard drive:*

1. Create a reference device with an operating system and the relevant software installed, including Network Agent and a security application.

2. Capture the reference image on the device and distribute that image on new devices through the dedicated task of Kaspersky Security Center Linux.

   To capture and install disk images, use third-party tools available in the organization.

### Copying a disk image with third-party tools

When applying third-party tools for capturing the image of a device with Network Agent installed, use one of the following methods:

- On the reference device, stop the Network Agent service and run the klmover utility with the `-dupfix` key. The utility klmover is included in the installation package of Network Agent. Avoid any subsequent runs of Network Agent service until the image capturing operation completes.
- Make sure that the klmover utility is run with the `-dupfix` key before the first run of the Network Agent service on target devices. This is a mandatory requirement and must be done at the first launch of the operating system after image deployment. The utility klmover is included in the installation package of Network Agent.
- Use the Network Agent disk cloning mode.

If the hard drive image has been copied incorrectly, you can resolve this problem.

You can also capture the image of a device without Network Agent installed. To do this, perform image deployment on target devices and then deploy Network Agent. If using this method, provide access to the network folder with stand-alone installation packages from a device.

## Network Agent disk cloning mode

Cloning the hard drive of a reference device is a popular method of software installation on new devices. If Network Agent is running in standard mode on the hard drive of the reference device, the following problem arises:

After the reference disk image with Network Agent is deployed on new devices, they are displayed in Kaspersky Security Center Web Console as a single device. This problem arises because the cloning procedure causes new devices to keep identical internal data, which allows the Administration Server to associate a device with its own record in Kaspersky Security Center Web Console.

The special *Network Agent disk cloning mode* allows you to avoid problems with an incorrect display of new devices in Kaspersky Security Center Web Console after cloning. Use this mode when you deploy software (with Network Agent) on new devices by cloning the disk.

In disk cloning mode, Network Agent keeps running but does not connect to the Administration Server. When exiting the cloning mode, Network Agent deletes the internal data, which causes Administration Server to associate multiple devices with a single record in Kaspersky Security Center Web Console. Upon completing the cloning of the reference device image, new devices are displayed in Kaspersky Security Center Web Console properly (under individual records).

### Network Agent disk cloning mode use scenario

1. The administrator installs Network Agent on the reference device.
2. The administrator checks the Network Agent connection to the Administration Server using the klnagchk utility.
3. The administrator enables the Network Agent disk cloning mode.

4. The administrator installs software and patches on the device, and restarts it as many times as needed.
5. The administrator clones the hard drive of the reference device on any number of devices.
6. Each cloned copy must meet the following conditions:
    a. The device name must be changed.
    b. The device must be restarted.
    c. The disk cloning mode must be disabled.

### Enabling and disabling the disk cloning mode using the klmover utility

*To enable or disable the Network Agent disk cloning mode:*

1. Run the klmover utility on the device with Network Agent installed that you have to clone.
   The klmover utility is located in the Network Agent installation folder.
2. To enable the disk cloning mode, enter the following command at the Linux command shell:
   `./klmover -cloningmode 1`
   Network Agent switches to disk cloning mode.
3. To request the current status of the disk cloning mode, enter the following command at the command prompt:
   `./klmover -cloningmode`
   The utility window shows whether the disk cloning mode is enabled or disabled.
4. To disable the disk cloning mode, enter the following command in the utility command line:
   `./klmover -cloningmode 0`

# Network Agent installation parameters

The table below describes the MSI properties that you can configure when installing Network Agent. All of the parameters are optional, except for EULA and SERVERADDRESS.

Parameters of Network Agent installation in silent mode

| MSI property | Description | Available values |
|---|---|---|
| EULA | Acceptance of the terms of the License Agreement | • 1—I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement.<br>• 0—I do not accept the terms of the License Agreement (installation is not performed).<br>• No value—I do not accept the terms of the License Agreement (installation is not performed). |
| DONT_USE_ANSWER_FILE | Read installation settings from response file | • 1—Do not use.<br>• Other value or no value—Read. |
| INSTALLDIR | Path to the Network Agent installation folder | String value. |
| SERVERADDRESS | Administration Server address (required) | String value. |

| MSI property | Description | Available values |
|---|---|---|
| SERVERPORT | Number of port for connection to Administration Server | Numerical value. |
| SERVERSSLPORT | Number of the port for encrypted connection to Administration Server by using SSL protocol | Numerical value. |
| USESSL | Whether to use SSL connection | • 1—Use.<br>• Other value or no value—Do not use. |
| OPENUDPPORT | Whether to open a UDP port | • 1—Open.<br>• Other value or no value—Do not open. |
| UDPPORT | UDP port number | Numerical value. |
| USEPROXY | Whether to use a proxy server. | • 1—Use.<br>• Other value or no value—Do not use. |
| PROXYLOCATION (PROXYADDRESS:PROXYPORT) | Proxy address and number of port for connection to proxy server | String value. |
| PROXYLOGIN | Account for connection to proxy server | String value. |
| PROXYPASSWORD | Password of account for connection to proxy server (Do not specify any details of privileged accounts in the parameters of installation packages.) | String value. |
| GATEWAYMODE | Connection gateway use mode | • 0—Do not use connection gateway.<br>• 1—Use this Network Agent as connection gateway.<br>• 2—Connect to the Administration Server using connection gateway. |
| GATEWAYADDRESS | Connection gateway address | String value. |
| CERTSELECTION | Method of receiving a certificate | • GetOnFirstConnection—Receive a certificate from the Administration Server.<br>• GetExistent —Specify an existing certificate. If this option is selected, the CERTFILE property must be defined. |
| CERTFILE | Path to the certificate file | String value. |
| VMVDI | Enable dynamic mode for Virtual Desktop Infrastructure (VDI) | • 1—Enable.<br>• 0—Do not enable.<br>• No value—Do not enable. |
| LAUNCHPROGRAM | Whether to start the Network Agent service after installation. The parameter is ignored if VMVDI=1 | • 1—Start.<br>• Other value or no value—Do not start. |
| NAGENTTAGS | Tag for Network Agent (has priority over the tag given in the response file) | String value. |

# Installing applications using a remote installation task

Kaspersky Security Center Linux allows you to install applications on devices remotely, using remote installation tasks. Those tasks are created and assigned to devices through a dedicated wizard. To assign a task more quickly and easily, you can specify devices (up to 1000 devices) in the wizard window in one of the following ways:

- **Assign task to an administration group**. In this case, the task is assigned to devices included in an administration group created earlier.
- **Specify device addresses manually or import addresses from a list**. You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.
- **Assign task to a device selection**. In this case, the task is assigned to devices included in a selection created earlier. You can specify the default selection or a custom one that you created. You can only select up to 1000 devices.

To avoid issues that may occur during installation of the application on a client device without Network Agent installed, you must proceed as described in forced deployment through the remote installation task of Kaspersky Security Center Linux.

## About remote installation tasks in Kaspersky Security Center Linux

Kaspersky Security Center Linux provides various mechanisms for remote installation of applications, which are implemented as remote installation tasks (forced installation, installation by copying a hard drive image). You can create a remote installation task both for a specified administration group and for specific devices or a selection of devices (such tasks are displayed in Kaspersky Security Center Web Console, in the **Tasks** folder). When creating a task, you can select installation packages (those of Network Agent and / or another application) to be installed within this task, as well as specify certain settings that define the method of remote installation. In addition, you can use the Remote installation wizard, which is based on creation of a remote installation task and results monitoring.

Tasks for administration groups affect both devices included in a specified group and all devices in all subgroups within that administration group. A task covers devices of secondary Administration Servers included in a group or any of its subgroups if the corresponding setting is enabled in the task.

Tasks for specific devices refresh the list of client devices at each run in accordance with the selection contents at the moment the task starts. If a selection includes devices that have been connected to secondary Administration Servers, the task will run on those devices, too. For details on those settings and installation methods see below in this section.

To ensure a successful operation of a remote installation task on devices connected to secondary Administration Servers, you must use the relaying task to relay installation packages used by your task to corresponding secondary Administration Servers in advance.

# Installing an application remotely

This section contains information on how to remotely install an application on devices in an administration group, devices with specific addresses, or a selection of devices.

*To install an application on specific devices:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts.
3. In the **Task type** field, select **Install application remotely**.
4. Choose one of the following options:

   **Assign task to an administration group**

   The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

   For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

   If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

   **Specify device addresses manually or import addresses from a list**

   You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

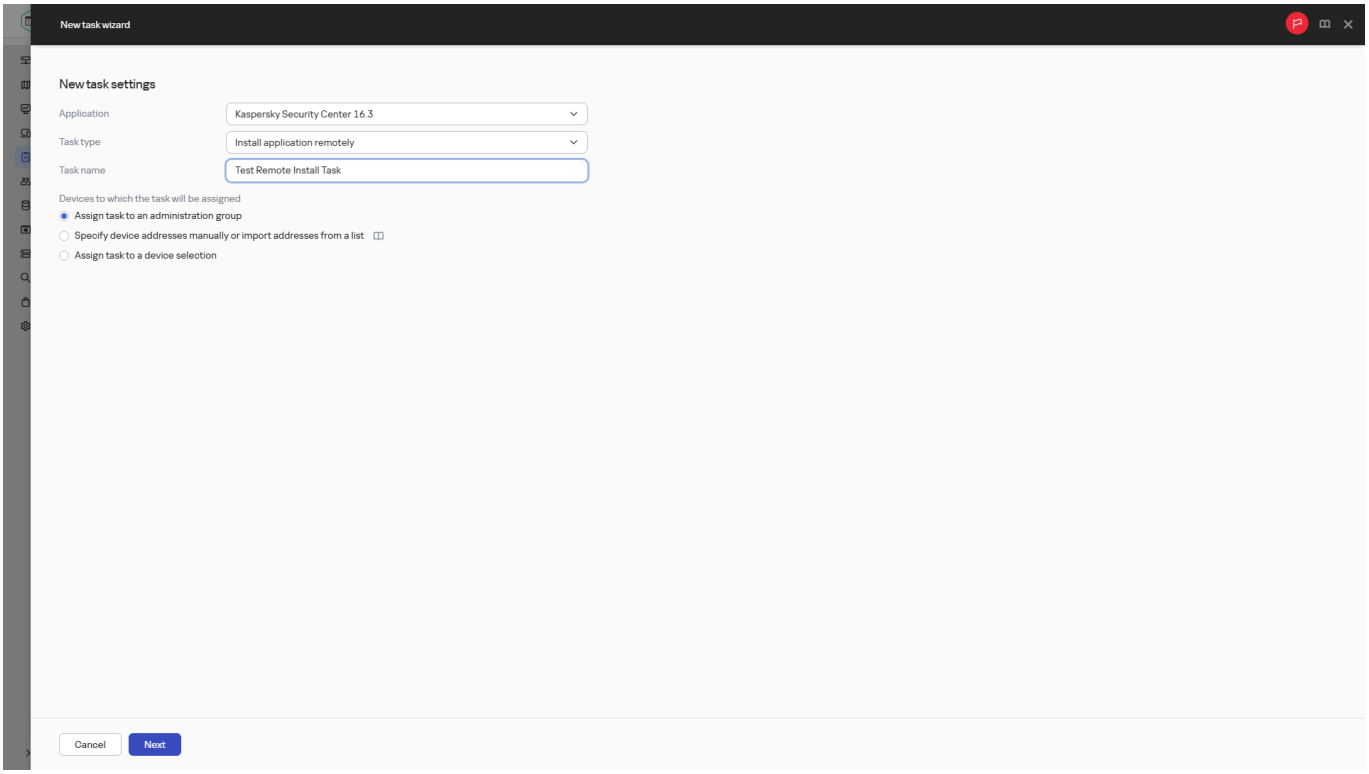
   You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

   **Assign task to a device selection**

   The task is assigned to devices included in a device selection. You can specify one of the existing selections.

   For example, you may want to use this option to run a task on devices with a specific operating system version.

The *Install application remotely* task is created for the specified devices. If you selected the **Assign task to an administration group** option, the task is a group one.




Creating the Install application remotely task

5. At the **Task scope** step, specify an administration group, devices with specific addresses, or a device selection.

   The available settings depend on the option selected at the previous step.

6. At the **Installation packages** step, specify the following settings:

   - In the **Select installation package** field, select the installation package of an application that you want to install.

   - In the **Force installation package download** settings group, specify how files that are required for the application installation are distributed to client devices:

     **Using Network Agent**

     If this option is enabled, installation packages are delivered to client devices by Network Agent installed on those client devices.

     If this option is disabled, installation packages are delivered using the operating system tools of client devices.

     We recommend that you enable this option if the task has been assigned to devices with Network Agents installed.

     By default, the option is enabled.

     **Using operating system resources through distribution points**

     If the check box is selected, the installation packages are delivered to client devices using the operating system's mechanisms through distribution point. You can select this option if there is at least one distribution point on the network.

     If the **Using Network Agent** option is enabled, the files are delivered using operating system tools only if Network Agent tools are unavailable.

By default, this option is enabled for remote installation tasks that have been created on a virtual Administration Server.

The only way to install an application for Windows (including Network Agent for Windows) on a device that does not have Network Agent installed is by using a Windows-based distribution point. Therefore, when you install a Windows application:

- Select this option.
- Ensure that a distribution point is assigned for the target client devices.
- Ensure the distribution point is Windows-based.

**Using operating system resources through Administration Server**

If this option is enabled, files are transmitted to client devices by using operating system tools of client devices through the Administration Server. You can enable this option if no Network Agent is installed on the client device, but the client device is in the same network as the Administration Server.

By default, the option is enabled.

- In the **Maximum number of concurrent downloads** field, specify the maximum allowed number of client devices to which Administration Server can simultaneously transmit the files.
- In the **Maximum number of installation attempts** field, specify the maximum allowed number of installer runs.

  If the number of attempts specified in the parameter is exceeded, Kaspersky Security Center Linux does not start the installer on the device anymore. To restart the *Install application remotely* task, increase the value of the **Maximum number of installation attempts** parameter and start the task. Alternatively, you can create a new *Install application remotely* task.
- If you migrate from one Kaspersky application to another and your current application is password-protected, enter the password in the **Password to uninstall the current Kaspersky application** field. Note that during the migration, your current Kaspersky application will be uninstalled.

  The **Password to uninstall the current Kaspersky application** field is only available if you have selected the **Using Network Agent** option in the **Force installation package download** settings group.

  You can use the uninstall password only for the Kaspersky Security for Windows Server to Kaspersky Endpoint Security for Windows migration scenario when installing Kaspersky Endpoint Security for Windows by using the Install application remotely task. Using the uninstall password when installing other components may cause installation errors.

  To complete the migration scenario successfully, make sure that the following prerequisites are met:

  - You are using Kaspersky Security Center Network Agent 14.2 for Windows or later.
  - You are installing the application on devices running Windows.
- Define the additional setting:

  **Do not re-install application if it is already installed**

  If this option is enabled, the selected application will not be re-installed if it has already been installed on this client device.

If this option is disabled, the application will be installed anyway.

By default, the option is enabled.

**Verify operating system type before downloading**

Before transmitting the files to client devices, Kaspersky Security Center Linux checks if the Installation utility settings are applicable to the operating system of the client device. If the settings are not applicable, Kaspersky Security Center Linux does not transmit the files and does not attempt to install the application. For example, to install some application to devices of an administration group that includes devices running various operating systems, you can assign the installation task to the administration group, and then enable this option to skip devices that run an operating system other than the required one.

When you remotely install Network Agent on unassigned devices, Kaspersky Security Center Linux or a distribution point automatically determines the device's operating system type, regardless of the **Verify operating system type before downloading** setting.

**Assign package installation in Active Directory group policies**

If this option is enabled, an installation package is installed by using the Active Directory group policies.

This option is available if the Network Agent installation package is selected.

By default, this option is disabled.

**Prompt users to close running applications**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

- Select on which devices you want to install the application:

  **Install on all devices**

  The application will be installed even on devices managed by other Administration Servers.

  This option is selected by default. You do not have to change this setting if you have only one Administration Server in your network.

  **Install only on devices managed through this Administration Server**

  The application will be installed only on devices managed by this Administration Server. Select this option if you have more than one Administration Server in your network and want to avoid conflicts between them.

- Specify whether devices must be moved to an administration group after installation:

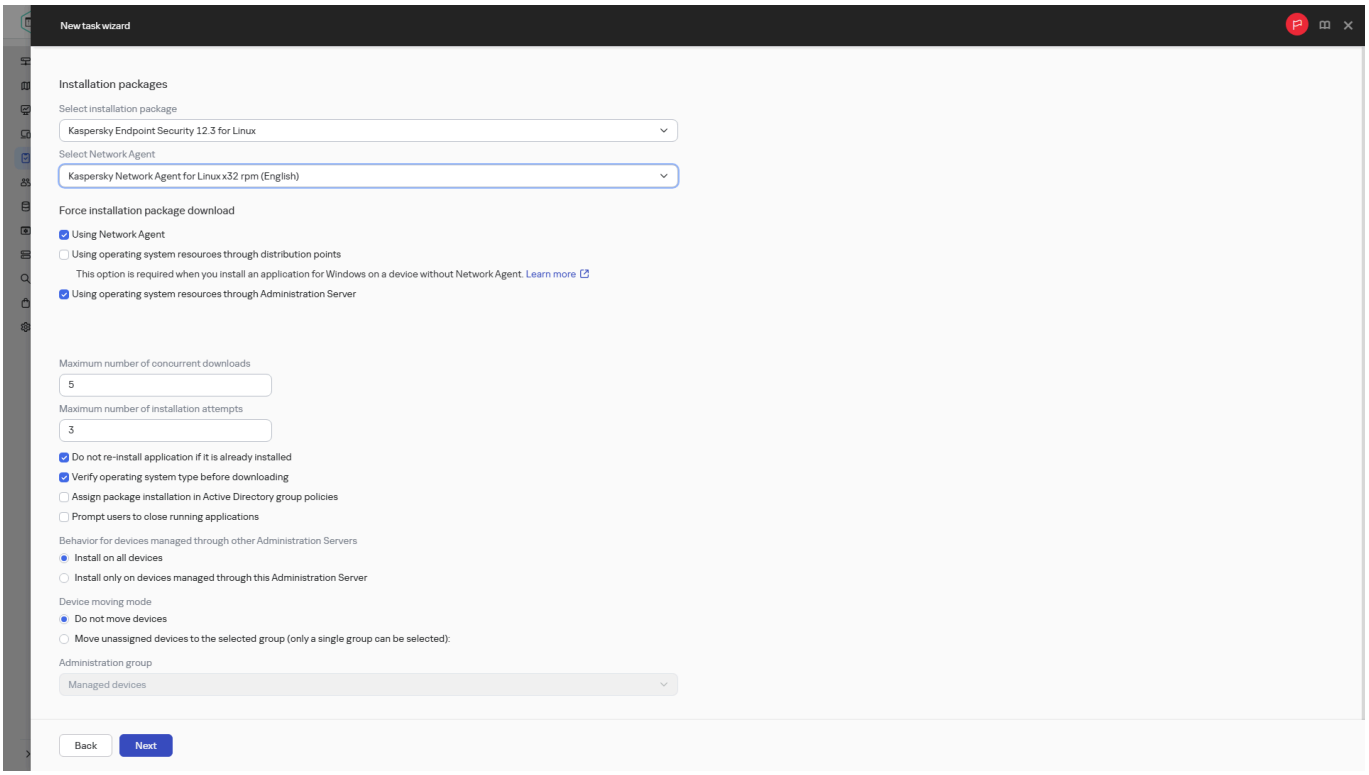
  **Do not move devices**

  The devices remain in the groups in which they are currently located. The devices that have not been placed in any group remain unassigned.

  **Move unassigned devices to the selected group (only a single group can be selected)**

  The devices are moved to the administration group that you select.

  Note that the **Do not move devices** option is selected by default. For security reasons, you might want to move the devices manually.




Specifying the task settings

7. At the this step of the wizard, specify whether the devices must be restarted during installation of applications:

   **Do not restart the device**

   If this option is selected, the device will not be restarted after the security application installation.

   **Restart the device**

   If this option is selected, the device will be restarted after the security application installation.

8. If necessary, at the **Select accounts to access devices** step, add the accounts that will be used to start the *Install application remotely* task:

   **No account required (Network Agent installed)**

   If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running.

   If Network Agent has not been installed on client devices, this option is not available.

   **Account required (Network Agent is not used)**

   Select this option if Network Agent is not installed on the devices for which you assign the remote installation task. In this case, you can specify a user account or an SSH certificate to install the application.

   - **Local or domain account**. If this option is selected, specify the user account under which the application installer will be run. Click the **Add** button, select **Local or domain account**, and then specify the user account credentials.

     You can specify multiple user accounts if, for example, none of them have all the required rights on all devices for which you assign the task. In this case, all added accounts are used for running the task, in consecutive order, top-down.

   - **SSH certificate**. If you want to install an application on a Linux-based client device, you can specify an SSH certificate instead of a user account. Click the **Add** button, select **SSH certificate**, and then specify the private and public keys of the certificate.

To generate a private key, you can use the ssh-keygen utility. Note that Kaspersky Security Center Linux supports the PEM format of private keys, but the ssh-keygen utility generates SSH keys in the OPENSSH format by default. The OPENSSH format is not supported by Kaspersky Security Center Linux. To create a private key in the supported PEM format, add the -m PEM option in the ssh-keygen command. For example:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
```

9. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

   If you enabled the **Open task details when creation is complete** option, the task settings window opens. In this window, you can check the task parameters, modify them, or configure a task start schedule, if necessary.

10. In the task list, select the task you created, and then click **Start**.

    Alternatively, wait for the task to launch according to the schedule that you specified in the task settings.

When the remote installation task is completed, the selected application is installed on the specified devices.

# Remote installing of applications on macOS devices

*To install applications on devices running macOS using a remote installation task:*

1. Create an archive that consists of an installation package and a .sh installation script.

2. Disable the **Verify operating system type before downloading** option in the New task wizard.

Alternatively, you can use the **Execute scripts remotely** task. The following article describes how to configure files for this task: Remotely installing applications on devices using the Execute scripts remotely task.

# Installing applications on secondary Administration Servers

If your Administration Server version is 15.4 or later, you can install applications on a secondary Administration Server only if its version is 15.4 or later.

*To install an application on secondary Administration Servers:*

1. Establish a connection with the Administration Server that controls the relevant secondary Administration Servers.

2. Make sure that the installation package corresponding to the application being installed is available on each of the selected secondary Administration Servers. If you cannot find the installation package on any of the secondary Servers, distribute it. For this purpose, create a task with the **Distribute installation package** task type.

3. Create a task for a remote application installation on secondary Administration Servers. Select the **Install application on secondary Administration Server remotely** task type.

   The New task wizard creates a task for remote installation of the application selected in the wizard on specific secondary Administration Servers.

4. Run the task manually or wait for it to launch according to the schedule that you specified in the task settings.

When the remote installation task is complete, the selected application is installed on the secondary Administration Servers.

# Remote installation of applications on devices with Network Agent installed

If an operable Network Agent connected to the primary Administration Server (or to any of its secondary Servers) is installed on a device, you can upgrade Network Agent on this device, as well as install, upgrade, or remove any supported applications through Network Agent.

You can enable the **Using Network Agent** option in the properties of the remote installation task.

If this option is selected, installation packages with installation settings defined by the administrator will be transferred to target devices over communication channels between Network Agent and the Administration Server.

To optimize the load on the Administration Server and minimize traffic between the Administration Server and the devices, it is useful to assign distribution points on every remote network or in every broadcasting domain (see sections "About distribution points" and "Building a structure of administration groups and assigning distribution points"). In this case, installation packages and the installer settings are distributed from the Administration Server to target devices through distribution points.

Moreover, you can use distribution points for broadcasting (multicast) delivery of installation packages, which allows reducing network traffic significantly when deploying applications.

When transferring installation packages to target devices over communication channels between Network Agents and the Administration Server, all installation packages that have been prepared for transfer will also be cached in the /var/opt/kaspersky/klnagent_srv/1093/.working/ folder. When using multiple large installation packages of various types and involving a large number of distribution points, the size of this folder may increase dramatically.

Files cannot be deleted from the FTServer folder manually. When original installation packages are deleted, the corresponding data will be automatically deleted from the FTServer folder.

The data received by distribution points is saved in the folder /var/opt/kaspersky/klnagent_srv/1103/.

Files cannot be deleted from the $FTClTmp folder manually. As tasks using data from this folder complete, the contents of this folder will be deleted automatically.

Because installation packages are distributed over communication channels between Administration Server and Network Agents from an intermediate repository in a format optimized for network transfers, no changes are allowed in installation packages stored in the original folder of each installation package. Those changes will not be automatically registered by Administration Server. If you need to modify the files of installation packages manually (although you are recommended to avoid this scenario), you must edit any of the settings of an installation package in Kaspersky Security Center Web Console. Editing the settings of an installation package in Kaspersky Security Center Web Console causes Administration Server to update the package image in the cache that has been prepared for transfer to target devices.

The server sends ICMP echo-requests (the same as the ping command) to the target device during remote installation.

# Managing device restarts in the remote installation task

Devices often need a restart to complete the remote installation of applications (particularly on Windows).

If you use the remote installation task of Kaspersky Security Center Linux, in the New task wizard or in the properties window of the task that has been created (**Operating system restart** section), you can select the action to perform when the Windows device requires a restart:

- **Do not restart the device**. In this case, no automatic restart will be performed. To complete the installation, you must restart the device (for example, manually or through the device management task). Information about the required restart will be saved in the task results and in the device status. This option is suitable for installation tasks on servers and other devices where continuous operation is critical.

- **Restart the device**. In this case, the device is always restarted automatically if a restart is required for completion of the installation. This option is useful for installation tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**. The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). The **Prompt user for action** is the most suitable for workstations where users need a possibility of selecting the most convenient time for a restart.

# Forced deployment through the remote installation task of Kaspersky Security Center Linux

To perform the initial deployment of Network Agent or other applications, you can force installation of selected installation packages by using the remote installation task of Kaspersky Security Center Linux—provided that each device has a user account(s) with local administrator rights.

Forced installation can also be applied if devices cannot be directly accessed by Administration Server: for example, devices are on isolated networks, or they are on a local network while the Administration Server item is in DMZ.

In case of initial deployment, Network Agent is not installed. Therefore, in the settings of the remote installation task, you cannot select distribution of files required for application installation by using Network Agent. You can only choose to distribute files by using operating system resources through Administration Server or distribution points.

The Administration Server service must run under an account that has administrative privileges on the target devices. Alternatively, you can specify an account that has access to the admin$ share in the settings of the remote installation task.

By default, the remote installation task is applied to devices by using the credentials of the account under which the Administration Server is running. It is important to clarify that this is the account used for accessing the admin$ share, rather than the account under which the remote installation task runs. Installation is carried out under the LocalSystem account.

You can specify target devices either explicitly (with a list), by selecting the Kaspersky Security Center Linux administration group to which they belong; or by creating a selection of devices based upon a specific criterion. The installation start time is defined by the task schedule. If the **Run missed tasks** setting is enabled in the task properties, the task can be run either immediately after target devices are turned on or when they are moved to the target administration group.

Forced installation consists of delivering installation packages to target devices, subsequent copying of files to the admin$ resource on each of the target devices, and remote registration of supporting services on those devices. Delivery of installation packages to target devices is performed through a Kaspersky Security Center Linux feature that ensures network interaction. The following conditions must be met in this case:

- Target devices are accessible from the Administration Server side or from the distribution point side.
- Name resolution for target devices functions properly on the network.
- The administrative shares (admin$) remain enabled on target devices.
- The following system services are running on target devices:
  - Server (LanmanServer)

    By default, this service is running.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- Port TCP 445 is open on target devices to enable remote access through Windows Management Instrumentation.

  TCP 139, UDP 137, and UDP 138 are used by older protocols and are no longer necessary for current applications.

  Dynamic outbound access ports must be allowed on the firewall for connections from the Administration Server and distribution points to target devices.
- The Active Directory domain policy security settings are allowed to provide the operation of the NTLM protocol during the deployment of Network Agent.
- On target devices running Microsoft Windows XP, Simple File Sharing mode is disabled.

- On target devices, the access sharing and security model are set as *Classic – local users authenticate as themselves*. It can in no way be *Guest only – local users authenticate as Guest*.
- Target devices are members of the domain, or uniform accounts with administrator rights are created on target devices in advance.

To successfully deploy Network Agent or other applications to a device that is not joined to a Windows Server 2003 or later Active Directory domain, you must disable remote UAC on that device. Remote UAC is one of the reasons that prevent local administrative accounts from accessing admin$, which is necessary for forced deployment of Network Agent or other applications. Disabling remote UAC does not affect local UAC.

During installation on new devices that have not yet been allocated to any of the Kaspersky Security Center Linux administration groups, you can open the remote installation task properties and specify the administration group to which devices will be moved after Network Agent installation.

When creating a group task, keep in mind that each group task affects all devices in all nested groups within a selected group. Therefore, you must avoid duplicating installation tasks in subgroups.

A simplified way to create tasks for forced installation of applications is automatic installation. To do this, you must open the administration group properties, open the list of installation packages, and then select the ones that must be installed on devices in this group. As a result, the selected installation packages will be automatically installed on all devices in this group and all of its subgroups. The time interval over which the packages will be installed depends on the network throughput and the total number of networked devices.

To reduce the load on Administration Server during the delivery of installation packages to target devices, you can select installation via distribution points in the installation task. Note that this installation method places a significant load on devices acting as distribution points. Therefore, it is recommended that you select devices that meet the requirements for distribution points. If you use distribution points, you have to make sure that they are present in each of the isolated subnets hosting target devices.

Using distribution points as local installation centers may also be useful when performing installation on devices in subnets communicated with Administration Server via a low-capacity channel while a broader channel is available between devices in the same subnet.

The free disk space in the partition with the /var/opt/kaspersky/KSC_Backups* folder must exceed, by many times, the total size of the distribution packages of installed applications.

# Installing applications in silent mode

*To install an application in silent mode:*

1. In the main menu, go to **Software management** → **Installation packages**.
2. Select the check box next to the installation package of the required application, or create a new one for that application.

   The installation package will be stored on the Administration Server in the Packages service folder that is in the shared folder. A separate subfolder corresponds to each installation package.

3. Open the folder storing the required installation package in one of the following ways:

   - By copying the folder corresponding to the relevant installation package from the Administration Server to the client device. Then open the copied folder on the client device.
   - By opening from the client device the shared folder that corresponds to the requisite installation package on the Administration Server.

   If the shared folder is located on a device that has Microsoft Windows Vista installed, you must set the **Disabled** value for the **User account control: Run all administrators in Admin Approval Mode** setting (**Start** → **Control Panel** → **Administration** → **Local security policy** → **Security settings**).

4. Depending on the selected application, do the following:

   - For Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers, and Kaspersky Security Center, navigate to the exec subfolder and run the executable file (the file with the .exe extension) with the /s key.
   - For other Kaspersky applications, run the executable file (a file with the .exe extension) with the /s key from the open folder.

   Running the executable file with the `EULA=1` and `PRIVACYPOLICY=1` keys means that you have fully read, understand and accept the terms of the End User License Agreement and the Privacy Policy, respectively. You are also aware that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. The text of the License Agreement and the Privacy Policy is included in the Kaspersky Security Center Linux distribution kit. Accepting the terms of the License Agreement and the Privacy Policy is necessary for installing the application or upgrading a previous version of the application.

# Preparing a macOS device for remote installation of Network Agent

There are the following methods to initially install Network Agent on the macOS managed device:

- By running the remote installation task on the macOS distribution point.
- By sending device users links to stand-alone packages generated by Kaspersky Security Center Linux. Stand-alone packages are executable modules that contain the distribution packages of selected applications with their settings defined.

*To prepare a device running macOS for remote installation of Network Agent:*

1. Make sure that sudo is installed on the target macOS device.
2. Test the device configuration:

   a. Make sure port 22 is open on the client device. To do this, in the **System Preferences**, open the **Sharing** pane, and then make sure the **Remote Login** check box is selected.

   You can connect to the client device via Secure Shell (SSH) only through port 22. You cannot change the port number.

You can use the `ssh <device_name>` command to log in to the macOS device remotely. In the **Sharing** pane, you can use the **Allow access for** option to set the scope of users who are allowed access to the macOS device.

b. Disable the sudo password for the user account under which the device is to be connected.

Use the `sudo visudo` command in the Terminal to open the sudoers configuration file. In the file that you have opened, in the `User privilege specification` entry specify the following: `username ALL = (ALL) NOPASSWD: ALL`. In this case, `username` stands for the user account, which is to be used for the device connection using SSH.

c. Save the sudoers file and then close it.

d. Connect to the device again through SSH and make sure that the Sudo service does not prompt you to enter a password; you can do this using the `sudo whoami` command.

3. Download and create an installation package:

a. Download the Network Agent installation package using one of the following methods:

- By using the application interface.
- By downloading the relevant version of Network Agent from Technical Support website at https://support.kaspersky.com/.
- By requesting the installation package from Technical Support specialists.

b. To create a remote installation package, use the following files:

- klnagent.kud
- install.sh
- klnagentmac.dmg

4. Create a remote installation task with the following settings:

- On the **Settings** page of the New task wizard, select the **Using operating system resources through Administration Server** check box. Clear all other check boxes.
- On the **Selecting an account to run the task** page, to run the task specify the settings of the user account that is used for device connection via SSH.

The client device is ready for remote installation of Network Agent through the corresponding task that you have created.

# Virtual infrastructure

Kaspersky Security Center Linux supports the use of virtual machines. You can install Network Agent and the security application on each virtual machine, and you can protect virtual machines at the hypervisor level. In the first case, you can use either a standard security application or Kaspersky Security for Virtualization Light Agent to protect your virtual machines. In the second case, you can use Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center Linux supports rollbacks of virtual machines to their previous state.

# Tips on reducing the load on virtual machines

When installing Network Agent on a virtual machine, you are advised to consider disabling some Kaspersky Security Center Linux features that seem to be of little use for virtual machines.

When installing Network Agent on a virtual machine or on a template intended for generation of virtual machines, we recommend the following actions:

- If you are running a remote installation, in the properties window of the Network Agent installation package, in the **Advanced** section, select the **Optimize settings for VDI** option.
- If you are running an interactive installation through a wizard, in the wizard window, select the **Optimize the Network Agent settings for the virtual infrastructure** option.

Selecting those options alters the settings of Network Agent so that the following features remain disabled by default (before a policy is applied):

- Retrieving information about software installed
- Retrieving information about hardware
- Retrieving information about vulnerabilities detected
- Retrieving information about updates required

Usually, those features are not necessary on virtual machines because they use uniform software and virtual hardware.

Disabling the features is invertible. If any of the disabled features is required, you can enable it through the policy of Network Agent, or through the local settings of Network Agent. The local settings of Network Agent are available through the context menu of the relevant device in Kaspersky Security Center Web Console.

# Support of dynamic virtual machines

Kaspersky Security Center Linux supports dynamic virtual machines. If a virtual infrastructure has been deployed on the organization's network, dynamic (temporary) virtual machines can be used in certain cases. The dynamic VMs are created under unique names based on a template that has been prepared by the administrator. The user works on a VM for a while and then, after being turned off, this virtual machine will be removed from the virtual infrastructure. If Kaspersky Security Center Linux has been deployed on the organization's network, a virtual machine with installed Network Agent will be added to the Administration Server database. After you turn off a virtual machine, the corresponding entry must also be removed from the database of Administration Server.

To make functional the feature of automatic removal of entries on virtual machines, when installing Network Agent on a template for dynamic virtual machines, select the **Enable dynamic mode for VDI** option:

- For remote installation—In the properties window of the installation package of Network Agent (**Advanced** section)
- For interactive installation—In the Network Agent installation wizard

Avoid selecting the **Enable dynamic mode for VDI** option when installing Network Agent on physical devices.

If you want events from dynamic virtual machines to be stored on the Administration Server for a while after you remove those virtual machines, then, in the Administration Server properties window, in the **Events repository** section, select the **Store events after devices are deleted** option and specify the maximum storage term for events (in days).

We do not recommend enabling drive encryption on dynamic virtual machines.

## Support of virtual machines copying

Copying a virtual machine with installed Network Agent or creating one from a template with installed Network Agent is identical to the deployment of Network Agents by capturing and copying a hard drive image. So, in general case, when copying virtual machines, you need to perform the same actions as when deploying Network Agent by copying a disk image.

However, the two cases described below showcase Network Agent, which detects the copying automatically. Owing to the above reasons, you do not have to perform the sophisticated operations described under "Deployment by capturing and copying the hard drive of a device":

- The **Enable dynamic mode for VDI** option was selected when Network Agent was installed—After each restart of the operating system, this virtual machine will be recognized as a new device, regardless of whether it has been copied or not.
- One of the following hypervisors is in use: VMware™, HyperV®, or Xen®: Network Agent detects the copying of the virtual machine by the changed IDs of the virtual hardware.

Analysis of changes in virtual hardware is not absolutely reliable. Before applying this method widely, you must test it on a small pool of virtual machines for the version of the hypervisor currently used in your organization.

# Specifying settings for remote installation on Unix devices

When you install an application on a Unix device by using a remote installation task, you can specify Unix-specific settings for the task. These settings are available in the task properties after the task is created.

*To specify Unix-specific settings for a remote installation task:*

1. In the main menu, go to **Tasks**.
2. Click the name of the remote installation task for which you want to specify the Unix-specific settings.

   The task properties window opens.
3. Go to **Application settings** → **Unix-specific settings**.
4. Specify the following parameters:

   **Set a password for the root account (only for deployment through SSH)**

   If the `sudo` command cannot be used on the target device without specifying the password, select this option, and then specify the password for the root account. Kaspersky Security Center Linux transmits the password in an encrypted form to the target device, decrypts the password, and then starts the installation procedure on behalf of the root account with the specified password.

   > Kaspersky Security Center Linux does not use the account or the specified password to create an SSH connection.

   **Specify the path to a temporary folder with Execute permissions on the target device (only for deployment through SSH)**

   If the /tmp directory on the target device does not have the execute permission, select this option, and then specify the path to the directory with the execute permission. Kaspersky Security Center Linux uses the specified directory as a temporary directory to access via SSH. The application places the installation package in the directory and runs the installation procedure.
5. Click the **Save** button.

The specified task settings are saved.

# Monitoring the deployment

To monitor the Kaspersky Security Center Linux deployment and make sure that a security application and Network Agent are installed on managed devices, use the monitoring and reporting feature:

- Use the deployment widget of the dashboard to monitor deployment in real time.
- Use reports to get detailed information.

# Starting and stopping Kaspersky applications

You can use the *Start or stop application* task for starting and stopping Kaspersky applications on managed devices.

*To create the Start or stop application task:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.
3. In the **Application** drop-down list, select the application for which you want to create the task.

   Kaspersky applications are displayed in the list if you have previously added management web plug-ins for these applications.
4. In the **Task type** list, select the **Application activation** task.
5. In the **Task name** field, specify the name of the new task.

   The task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).
6. Select devices to which the task will be assigned.
7. In the **Applications** window, do the following:
   - Select the check boxes next to the names of applications for which you want to create the task.
   - Select the **Start application** or the **Stop application** option.
8. If you want to modify the default task settings, enable the **Open task details when creation is complete** option at the **Finish task creation** step. If you do not enable this option, the task is created with the default settings. You can change the default settings later, at any time.
9. Click the **Finish** button.

   The task is created and displayed in the list of tasks.
10. Click the name of the created task to open the task properties window.
11. In the task properties window, specify the general task settings according to your needs, and then save the settings.

The task is created and configured.

If you want to run the task, select it in the task list, and then click the **Start** button.

# Replacing third-party security applications

Installation of Kaspersky security applications through Kaspersky Security Center Linux may require removal of third-party software that is incompatible with the application being installed. Kaspersky Security Center Linux provides several ways of removing the third-party applications.

### Removing incompatible applications when configuring remote installation of an application

You can enable the **Uninstall incompatible applications automatically** option when you configure remote installation of a security application in the Protection deployment wizard. When this option is enabled, Kaspersky Security Center Linux removes incompatible applications before installing a security application on a managed device.

### Removing incompatible applications through a dedicated task

To remove incompatible applications through a task, use the *Uninstall application remotely.* This task should be run on devices before the security application installation task. For example, in the installation task you can select **On completing another task** as the schedule type where the other task is *Uninstall application remotely*.

This method of uninstallation is useful when the security application installer cannot properly remove an incompatible application.

# Removing applications or software updates remotely

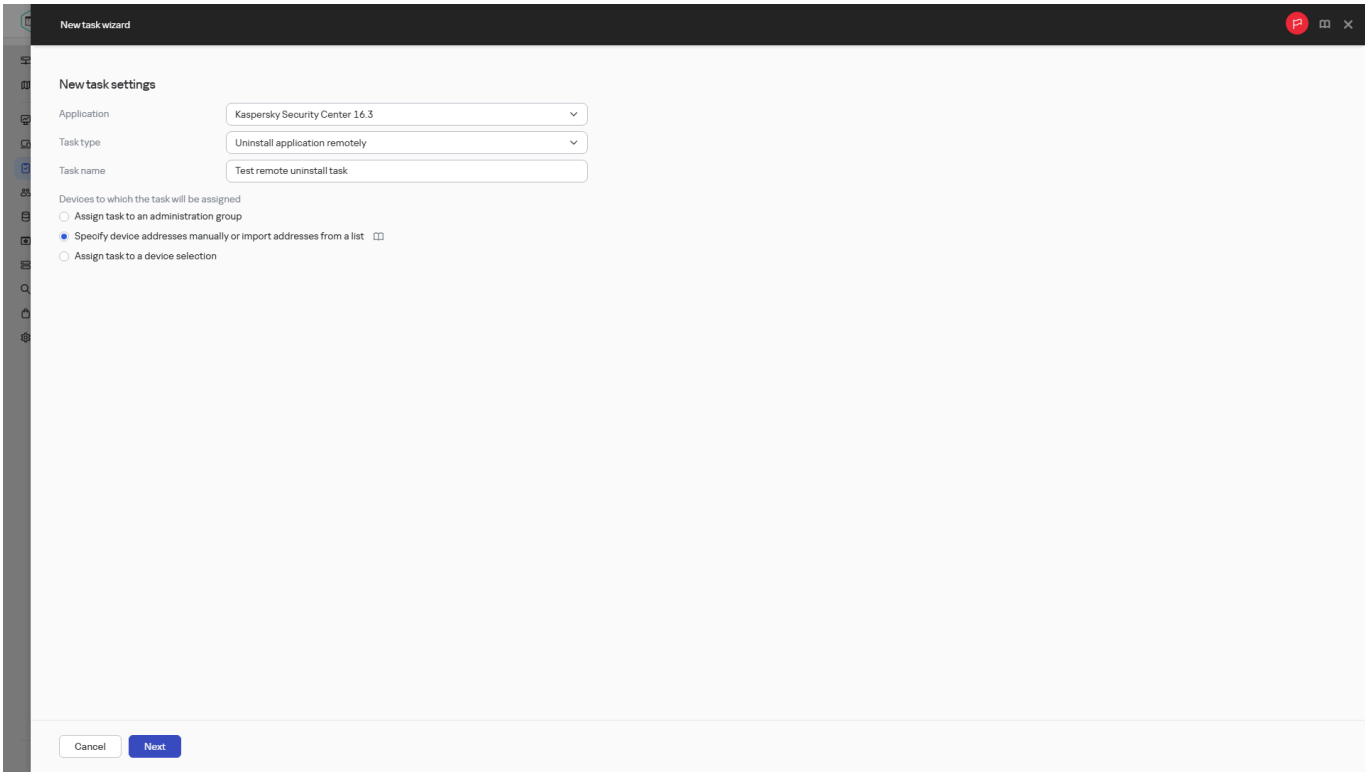
You can remove applications or software updates on managed devices that run Linux remotely only by using Network Agent.

*To remove applications or software updates remotely from selected devices:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.
3. In the **Application** drop-down list, select Kaspersky Security Center Linux.
4. In the **Task type** list, select the **Uninstall application remotely** task type.
5. In the **Task name** field, specify the name of the new task.

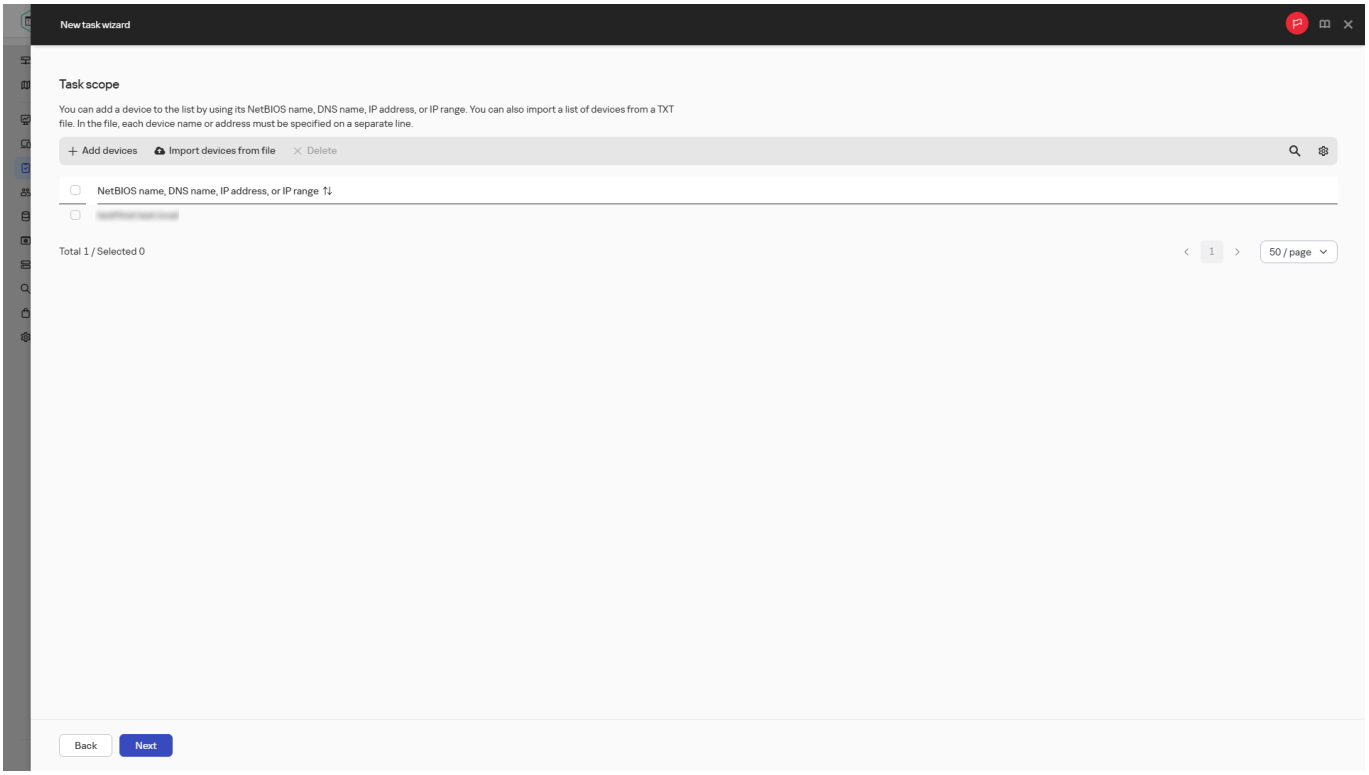
The task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).




Creating the Uninstall application remotely task

6. Select devices to which the task will be assigned.

   Go to the next step of the wizard.




Specifying the task scope

7. Select what kind of software you want to remove, and then select specific applications, updates, or patches that you want to remove:

   **Uninstall managed application**

   A list of Kaspersky applications is displayed. Select the application that you want to remove.

**Uninstall incompatible application**

A list of applications incompatible with Kaspersky security applications or Kaspersky Security Center Linux is displayed. Select the check boxes next to the applications that you want to remove.

**Uninstall application from applications registry**

By default, Network Agents send the Administration Server information about the applications installed on the managed devices. The list of installed applications is stored in the applications registry.

*To select an application from the applications registry:*

a. Click the **Application to uninstall** field, and then select the application that you want to remove.

> If you select Kaspersky Security Center Network Agent, when you run the task, the status *Completed successfully* shows that the process of removing started. If Kaspersky Security Center Network Agent is removed, the status does not change. If the task fails, the status changes to *Failed.*

b. Specify the uninstallation options:

- **Uninstallation mode**

  Select how you want to remove the application:

  - **Define uninstallation command automatically**

    If the application has an uninstallation command defined by the application vendor, Kaspersky Security Center Linux uses this command. We recommend that you select this option.

  - **Specify uninstallation command**

    Select this option if you want to specify your own command for the application uninstallation.

    > We recommend that you first try to remove the application by using the **Define uninstallation command automatically** option. If the uninstallation through the automatically defined command fails, then use your own command.

    Type an installation command into the field, and then specify the following option:

    **Use this command for uninstallation only if the default command was not autodetected**

    Kaspersky Security Center Linux checks whether or not the selected application has an uninstallation command defined by the application vendor. If the command is found, Kaspersky Security Center Linux will use it instead of the command specified in the **Command for application uninstallation** field.

    We recommend that you enable this option.

- **Perform restart after successful application uninstallation**

  If the application requires the operating system to be restarted on the managed device after successful uninstallation, the operating system is restarted automatically.

**Uninstall the specified application update, patch, or third-party application**

A list of updates, patches, and third-party applications is displayed. Select the item that you want to remove.

The displayed list is a general list of applications and updates, and it does not correspond to the applications and updates installed on the managed devices. Before selecting an item, we recommend that you ensure that the application or update is installed on the devices defined in the task scope. You can view the list of devices on which the application or update is installed, via the properties window.

*To view the list of devices:*

a. Click the name of the application or update.

The properties window opens.

b. Open the **Devices** section.

You can also view the list of installed applications and updates in the device properties window.

8. Specify how client devices will download the Uninstallation utility:

**Using Network Agent**

The files are delivered to client devices by Network Agent installed on those client devices.

If this option is disabled, the files are delivered using the Linux operating system tools.

We recommend that you enable this option if the task has been assigned to devices with Network Agents installed.

**Using operating system resources through Administration Server**

The option is obsolete. Use the **Using Network Agent** or **Using operating system resources through distribution points** option instead.

The files are transmitted to client devices by using the Administration Server operating system tools. You can enable this option if no Network Agent is installed on the client device, but the client device is in the same network as the Administration Server.

**Using operating system resources through distribution points**

The files are transmitted to client devices by using operating system tools through distribution points. You can enable this option if there is at least one distribution point on the network.

If the **Using Network Agent** option is enabled, the files are delivered by using operating system tools only if Network Agent tools are unavailable.

**Maximum number of concurrent downloads**

The maximum allowed number of client devices to which Administration Server can simultaneously transmit the files. The larger this number, the faster the application will be uninstalled, but the load on Administration Server is higher.

**Maximum number of uninstallation attempts**

If, when running the *Uninstall application remotely* task, Kaspersky Security Center Linux fails to uninstall the application on a managed device within the number of installer runs specified by the parameter, Kaspersky Security Center Linux stops delivering the uninstallation utility to this managed device and does not start the installer on the device anymore.

The **Maximum number of uninstallation attempts** parameter allows you to save the resources of the managed device, as well as reduce traffic (uninstallation, MSI file run, and error messages).

Recurring task start attempts may indicate a problem on the device and which prevents uninstallation. The administrator should resolve the problem within the specified number of uninstallation attempts and then restart the task (manually or by a schedule).

If uninstallation is not achieved eventually, the problem is considered unresolvable and any further task starts are seen as costly in terms of unnecessary consumption of resources and traffic.

When the task is created, the counter of attempts is set to `0`. Each run of the installer that returns an error on the device increments the counter reading.

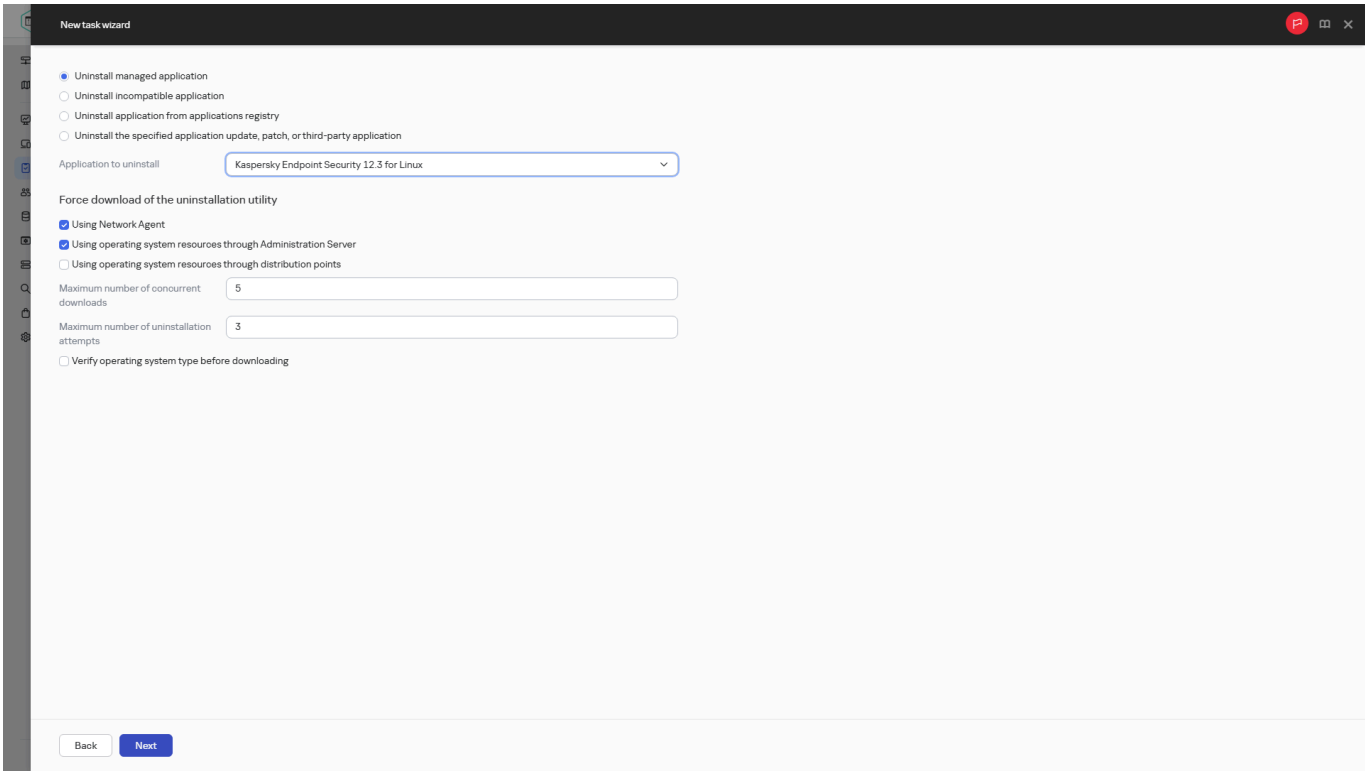
If the number of attempts specified in the parameter has been exceeded and the device is ready for application uninstallation, you can increase the value of the **Maximum number of uninstallation attempts** parameter and start the task to uninstall the application. Alternatively, you can create a new *Uninstall application remotely* task.

**Verify operating system type before downloading**

Before transmitting the files to client devices, Kaspersky Security Center Linux checks if the Installation utility settings are applicable to the operating system of the client device. If the settings are not applicable, Kaspersky Security Center Linux does not transmit the files and does not attempt to install the application. For example, to install some application to devices of an administration group that includes devices running various operating systems, you can assign the installation task to the administration group, and then enable this option to skip devices that run an operating system other than the required one.

When you remotely install Network Agent on unassigned devices, Kaspersky Security Center Linux or a distribution point automatically determines the device's operating system type, regardless of the **Verify operating system type before downloading** setting.

Go to the next step of the wizard.




Specifying the task settings

9. Specify the operating system restart settings:

**Do not restart the device**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

**Restart the device**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

**Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**
- **Restart after (min)**

**Force closure of applications in blocked sessions**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

Go to the next step of the wizard.

10. If necessary, add the accounts that will be used to start the remote uninstallation task:

**No account required (Network Agent installed)**

If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running.

If Network Agent has not been installed on client devices, this option is not available.

**Account required (Network Agent is not used)**

Select this option if Network Agent is not installed on the devices for which you assign the *Uninstall application remotely* task. In this case, you can specify a user account or an SSH certificate to uninstall the application.

- **Local or domain account**. If this option is selected, specify the user account under which the application installer will be run. Click the **Add** button, select **Local or domain account**, and then specify the user account credentials.

  You can specify multiple user accounts if, for example, none of them have all the required rights on all devices for which you assign the task. In this case, all added accounts are used for running the task, in consecutive order, top-down.

- **SSH certificate**. If you want to uninstall an application from a Linux-based client device, you can specify an SSH certificate instead of a user account. Click the **Add** button, select **SSH certificate**, and then specify the private and public keys of the certificate.

  To generate a private key, you can use the ssh-keygen utility. Note that Kaspersky Security Center Linux supports the PEM format of private keys, but the ssh-keygen utility generates SSH keys in the OPENSSH format by default. The OPENSSH format is not supported by Kaspersky Security Center Linux. To create a private key in the supported PEM format, add the -m PEM option in the ssh-keygen command.

  For example:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<user email>"
  ```

11. If at the **Finish task creation** step of the wizard, you enable the **Open task details when creation is complete** option, you can edit the default settings of the task.

    If you do not enable this option, the task is created with the default settings. You can modify the default settings later.

12. Click the **Finish** button.

    The wizard creates the task. If you enabled the **Open task details when creation is complete** option, the task properties window automatically opens. In this window, you can specify the general task settings and, if required, change the settings specified during task creation.

    > You can also open the task properties window by clicking the name of the created task in the list of tasks.

    The task is created, configured, and displayed in the list of tasks at **Tasks**.

13. To run the task, select it in the task list, and then click the **Start** button.

    You can also set a task start schedule on the **Schedule** tab of the task properties window.

    For a detailed description of scheduled start settings, refer to the general task settings.

After the task is completed, the selected application is removed from the selected devices.

## Remote uninstallation issues

Sometimes remote uninstallation of third-party applications may finish with the following warning: "Remote uninstallation has finished on this device with warnings: Application for removal is not installed." This issue occurs when the application to be uninstalled has already been uninstalled or was installed only for an individual user. Applications installed for an individual user (also referred to as per-user applications) become invisible and cannot be uninstalled remotely if the user is not logged in.

This behavior differs from applications intended for use by multiple users on the same device (also referred to as per-device applications). Per-device applications are visible and accessible to all users of the device.

Therefore, per-user applications must be uninstalled only when the user is logged in.

## Source of information about installed applications

The Network Agent retrieves information about software installed on Windows devices from the following registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contains information about applications installed for all users.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Contains information about applications installed for all users.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contains information about applications installed for the current user.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contains information about applications installed for specific users.

# Preparing a Windows device for remote installation

Remote installation of the application on the client device may return an error for the following reasons:

- The task has already been successfully performed on this device.

  In this case, the task does not have to be performed again.

- When a task was started, the device was shut down.

  In this case, turn on the device, and then restart the task.

- There is no connection between the Administration Server and the Network Agent installed on the client device.

  To determine the cause of the problem, use the utility designed for remote diagnostics of client devices (klactgui).

- If Network Agent is not installed on the device, the following issues may occur during remote installation:

  - The client device has **Disable simple file sharing** option enabled.
  - The Server service is not running on the client device.
  - The required ports are closed on the client device.
  - The account that is used to perform the task has insufficient privileges.

  To avoid issues that may occur during installation of the application on a client device without Network Agent installed, you must proceed as described in forced deployment through the remote installation task of Kaspersky Security Center Linux.

Previously, the riprep utility was used to prepare a device for remote installation. This is now considered an outdated method for configuring operating systems. The riprep utility is not recommended for use on operating systems newer than Windows XP and Windows Server 2003 R2.

# Creating Execute scripts remotely task

You can create an *Execute scripts remotely* task to execute an installation package on a client device and to remotely install an application.

An installation package contains a ZIP archive with a set of scripts for execution on client devices as well as a manifest.json file. Learn more about creating this type of installation package this article.

This task must be started only on devices with Network Agent for Linux.

*To start an Execute scripts remotely task:*

1. Go to the **New task wizard** and select the **Execute scripts remotely** task type.
2. Enter the task name and select the devices the task will be assigned to. Click **Next**.
3. Select an installation package based on a ZIP archive with a manifest.json file for remote execution.

   If you do not want to rerun the task on devices where it has already completed, turn on the **Do not start this task on devices on which it has already been completed** option.
4. Select an account to run the task.

   If you select the default account, the task will be performed by the Network Agent (root account).

   > When the *Execute scripts remotely* task starts, you cannot change the account it is assigned to. To change the account the task is assigned to, stop the task in the task settings and create it again with the correct account details.
5. If you want to modify the default task settings, enable the **Open task details when creation is complete** option on the **Finish task creation** page. If you do not enable this option, the task is created with the default settings. You can change the default settings later, at any time.
6. Click the **Finish** button.

   The *Execute scripts remotely* task is created and appears in the list of tasks.

> After receiving data from the *Execute scripts remotely* task, Network Agent restricts access to the received data for all users, except the administrator and the user specified in the task settings.

# Creating an installation package based on a manifest file

*To create an installation package based on a manifest file:*

1. In the main menu, go to **Software management → Installation packages**.

   A list of installation packages available on the Administration Server is displayed.
2. Click **Add**.

   The New package wizard starts. Proceed through the wizard by using the **Next** button.
3. Select **Create an installation package for the Execute scripts remotely task based on a ZIP archive with the manifest.json file**.
4. Specify the package name and click the **Browse** button.

   In the window that opens, choose a file to create the installation package.
5. Select an archive file located on the available disks. Learn how to prepare an archive for this task in this article.

   The file begins to upload to the Kaspersky Security Center Linux Administration Server.

   The process to create the installation package is started.

   The wizard informs you when the process is finished.

If the installation package is not created, an appropriate message is displayed.

6. Click the **Finish** button to close the wizard.

The installation package that you created is downloaded to the Packages subfolder of the Administration Server shared folder. After downloading, the installation package appears in the list of installation packages.

In the list of installation packages available on Administration Server, by clicking the link with the name of a custom installation package, you can:

- View the following properties of an installation package:
  - **Name.** Custom installation package name.
  - **Source.** Application vendor name.
  - **Version.** Application version.
  - **Created.** Installation package creation date.
  - **Modified.** Installation package modification date.
  - **Path.** Path to the custom installation package on the Administration Server.
- Change the package name and command-line parameters. This feature is available only for packages that are not created based on Kaspersky applications.

# Preparing an archive for Execute scripts remotely task

An archive for the *Execute scripts remotely* task based on a manifest.json file must meet the following requirements:

- Archive format: ZIP.
- Total size: no more than 1 GB.
- The number of files and folders in the archive is unlimited.
- The manifest file for the archive must match the schema below and must be named manifest.json. The schema is validated only during task execution on a device.

  **JSON schema of the manifest file and description of arrays**

  JSON schema

```
{
 "$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"
    ]
}
```

Example of the manifest file

```
{
  "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"
    }
  ]
}
```

- The archive must be structured as follows:

```
manifest.json
<file1>
<file2>
<folder1>/<file3>
<folder2>/<folder3>/<file4>
...
<fileX>
```

`manifest.json` is the manifest file for the task.

`<file1>`, ..., `<fileX>` is the set of files with scripts to be executed.

# Remotely installing applications on devices using the Execute scripts remotely task

The *Execute scripts remotely* task can be used to remotely install an application on a client device by creating a custom installation package.

Learn how to prepare an archive for this task in this article.

To create an installation package for remote installation of an application on a client device, the following files must be included in the archive you want to upload for this task:

- `<package name>.deb`
- **install.sh**

  `sudo apt-get install <package name>.deb`
- **manifest.json**

JSON schema for remote installation of an application

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<enter the arguments, if necessary>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

Description of arrays

1. `version`—version of the manifest file and the task.

   At present, the only acceptable value is 1.

2. The elements of the `actions` array determine the composition and order of the scripts that are executed in the task.

   The order of execution of the script corresponds to an element's index (place) in the array.

3. For each element of the `actions` array, the following elements are defined.

    a. `type`—type of executable command from scripts. At present, the value is always `execute`.

    b. `path`—path to the script file in the archive.

    c. `args`—arguments that are passed to the script as part of the executable command.

    d. `results`—array that defines further actions depending on the result of the task.

        1. `code`—value that returns a script.

        2. `next`—action to be completed next. The `continue` action proceeds to execute the next script (element in the `actions` array). The `break` action stops the task.

    e. `default_next`—action if a script returns a value that is not contained in `results`.

When the *Execute scripts remotely* task starts, the Network Agent will upload the installation package with the application to the client device. When the client device receives the installation package, Network Agent on this device parses the manifest.json file and defines the execution order of scripts and actions depending on the result and then starts execution.

When the *Execute scripts remotely* task is completed, the application will be installed on the client device.

# Configuring notifications and monitoring for the Execute scripts remotely task

You can configure monitoring, event-saving behavior, and notifications for the *Execute scripts remotely* task.

*To view the status of the Execute scripts remotely:*

1. In the main menu, go to **Tasks**.

   The list of tasks is displayed.

2. Select the task and click **Device history**.

   The progress of the task is shown.

*To configure the event-saving behavior:*

1. In the list of tasks, click on the task and go to the **Settings** tab.

2. In the **Notifications** section, click the **Settings** button.

3. Select one of the following options for how the application behaves after the task is complete:

   - **Save all events**.
   - **Save events related to task progress**.
   - **Save only task execution results**.

     The events are saved in the **Device history** and **Events repository**.

By default, only the task execution results are saved.

> If you select **Save all events**, only the task execution results will be saved.

4. If you want to keep the events in the Administration Server database, in the event log on the Administration Server, or on the device, turn on the corresponding option.

Learn more about configuring notifications in this article.

# Licensing

This section provides the following information:

- General concepts related to Kaspersky Security Center Linux licensing
- Instructions on license management of managed Kaspersky applications

# Licensing of Kaspersky Security Center Linux

This section describes general concepts related to Kaspersky Security Center Linux licensing.

## About the End User License Agreement

*The End User License Agreement* (License Agreement or EULA) is a binding agreement between you and AO Kaspersky Lab stipulating the terms under which you may use the application.

Carefully read the License Agreement before you start using the application.

Kaspersky Security Center Linux and its components, for example, Network Agent, have their own EULA.

You can view the terms of the End User License Agreement for Kaspersky Security Center Linux by using the following methods:

- During installation of Kaspersky Security Center.
- By reading the license.txt document included in the Kaspersky Security Center distribution kit.
- By reading the license.txt document in the Kaspersky Security Center installation folder.
- By downloading the license.txt file from the Kaspersky website.

You can view the terms of the End User License Agreement for Network Agent for Linux by using the following methods:

- While downloading the Network Agent distribution package from the Kaspersky web servers.
- During installation of Network Agent for Linux.
- By reading the license.txt document included in the Network Agent for Linux distribution package.
- By reading the license.txt document in the Network Agent for Linux installation folder.
- By downloading the license.txt file from the Kaspersky website.

You accept the terms of the End User License Agreement by confirming that you agree with the End User License Agreement when installing the application. If you do not accept the terms of the License Agreement, cancel the application installation and do not use the application.

# About the license

A *license* is a time-limited right to use Kaspersky Security Center, granted under the terms of the signed License Contract (End User License Agreement).

The scope of services and validity period depend on the license under which the application is used.

The following license types are provided:

- *Trial*

  A free license intended for trying out the application. A trial license usually has a short term.

  When a trial license expires, all Kaspersky Security Center Linux features become disabled. To continue using the application, you need to purchase a commercial license.

  You can use the application under a trial license for only one trial period.

- *Commercial*

  A paid license.

  When a commercial license expires, key features of the application become disabled. To keep Kaspersky Security Center working, you must renew your commercial license. After the license expires, you may no longer use the application and must delete it from the device.

  We recommend renewing your license before it expires, to ensure uninterrupted protection against all security threats.

# About the License Certificate

A *License Certificate* Is a document that is provided to you along with a key file or activation code.

The License Certificate contains the following information about the license being granted:

- License ID or order number
- Information about the user who is granted the license
- Information about the application that can be activated under the license provided
- Limit of the number of licensing units (e.g., devices on which the application can be used under the license provided)
- Start date of the license term
- License expiration date or license term
- License type

# About the license key

A *license key* is a sequence of bits that you can apply to activate and then use the application in accordance with the terms of the End User License Agreement. License keys are generated by Kaspersky specialists.

You can add a license key to the application using one of the following methods: by applying a *key file* or by entering an *activation code*. The license key is displayed in the application interface as a unique alphanumeric sequence after you add it to the application.

The license key may be blocked by Kaspersky in case the terms of the License Agreement have been violated. If the license key has been blocked, you need to add another one if you want to use the application.

A license key may be active or additional (or reserve).

An *active license key* is a license key that is currently used by the application. An active license key can be added for a trial or commercial license. The application cannot have more than one active license key.

An *additional (or reserve) license key* is a license key that entitles the user to use the application, but is not currently in use. The additional license key automatically becomes active when the license associated with the current active license key expires. An additional license key can be added only if an active license key has already been added.

A license key for a trial license can be added as an active license key. A license key for a trial license cannot be added as an additional license key.

# Viewing the Privacy Policy

The Privacy Policy is available online at https://www.kaspersky.com/products-and-services-privacy-policy.

The Privacy Policy is also available offline:

- You can read the Privacy Policy before Installing Kaspersky Security Center Linux.
- The Privacy Policy text is included in the license.txt file, in the Kaspersky Security Center Linux installation folder.
- The privacy_policy.txt file is available on a managed device, in the Network Agent installation folder.
- You can unpack the privacy_policy.txt file from the Network Agent distribution package.

# Kaspersky Security Center licensing options

Kaspersky Security Center can work in the following modes:

- **Basic functionality of Administration Console**

  Kaspersky Security Center works in this mode before the application is activated or after the commercial license expires. Kaspersky Security Center with support of the basic functionality of Administration Console is delivered as a part of Kaspersky applications for protection of corporate networks. You can also download it from Kaspersky website.

- **Commercial license**

  If you need additional functionality which is not included in the basic functionality of Administration Console, you must purchase a commercial license.

  When adding a license key in the Administration Server properties window, ensure that you add a license key that lets you use Kaspersky Security Center Linux. You can find this information at the Kaspersky website. Each solution webpage contains the list of applications included in this solution. Administration Server may accept unsupported license keys, for example a license key for Kaspersky Endpoint Security Cloud, but such license keys provide no new features in addition to the basic functionality of Administration Console.

| Feature or property | Kaspersky Security Center Linux operation mode | |
|---|---|---|
| | License is missing | Commercial license |
| **Basic functionality of Administration Console**<br>The following functions are available:<br>• Creation of virtual Administration Servers that are used to administer a network of remote offices or client organizations.<br>• Creation of a hierarchy of administration groups to manage specific devices as a single entity.<br>• Remote installation of applications.<br>• Centralized configuration of applications installed on client devices.<br>• Control of the anti-virus security status of an organization.<br>• Management of user roles.<br>• Statistics and reports on the application's operation, as well as notifications about critical events.<br>• Centralized operations with files that were moved to Quarantine or Backup and files whose processing was postponed.<br>• Encryption and data protection management.<br>• Viewing and manual editing of the list of hardware components detected by polling the network.<br>• Viewing the list of operating system images available for remote installation. | ✓ | ✓ |
| **Vulnerability and patch management: basic functionality**<br>The following tasks do not require a commercial license:<br>• The *Find vulnerabilities and required updates* task<br>Through this task, Kaspersky Security Center Linux receives the lists of detected vulnerabilities and required updates for the third-party software installed on the managed devices.<br>• The *Fix vulnerabilities* task<br>The *Fix vulnerabilities* task uses the recommended fixes for Microsoft software and user fixes for third-party software. To use this task, you must manually specify user fixes for vulnerabilities in the task settings. | ✓ | ✓ |

| Feature or property | Kaspersky Security Center Linux operation mode | |
|---|---|---|
| | License is missing | Commercial license |
| **Vulnerability and patch management: advanced functionality**<br>You can define the rules for automatic remote installation of software updates and fixing of vulnerabilities automatically. | — | ✓ |
| **Systems management**<br>The following functions are available:<br>• Remote permission of connection to client devices through a component of Microsoft® Windows® named Remote Desktop Connection.<br>• Remote connection to client devices through Windows Desktop Sharing. | — | ✓ |
| **Exporting events to SIEM systems: using the Syslog protocol**<br>Using the Syslog protocol, you can relay any events that occur on the Kaspersky Security Center Administration Server and in Kaspersky applications that are installed on managed devices. The Syslog protocol is a standard message-logging protocol. You can use it to export events to any SIEM system. | ✓ | ✓ |
| Aggregating alerts and performing response actions through Active directory, KASAP, and Kaspersky TIP Sandbox | — | ✓ |

# About the key file

A *key file* is a file with the .key extension provided to you by Kaspersky. Key files are designed to activate the application by adding a license key.

You receive a key file at the email address that you provided when you bought Kaspersky Security Center or ordered the trial version of Kaspersky Security Center.

You do not need to connect to Kaspersky activation servers in order to activate the application with a key file.

If the key file has been accidentally deleted, you can restore it. You may need a key file, for example, to register with Kaspersky CompanyAccount.

To restore the key file, you need to do one of the following:

- Contact the license seller.
- Get a key file on the Kaspersky website based on the available activation code.

# About data provision

## Data provided to third parties

When using the Mobile Device Management functionality of the Software, for the purpose of timely delivery of commands to devices running the Android operating system through the push notification mechanism, the Google Firebase Cloud Messaging service is used. If the User has configured the usage of the Google Firebase Cloud Messaging service, the User agrees to provide the following information to the Google Firebase Cloud Messaging service in automatic mode:

- Instance ID
- Software ID in the Google Firebase Cloud Messaging service
- Version of the installed software
- Full version of the Software
- Google Play version
- Software distributive package name
- Schema version for data provided
- Operating system version
- Software ID

To block exchange of information with the Google Firebase Cloud Messaging service, the User must roll back the usage settings of the Google Firebase Cloud Messaging service to their factory values.

When using the Mobile Device Management functionality of the Software, for the purpose of timely delivery of commands to devices running the iOS operating system through the push notification mechanism, the Apple Push Notification Service (APNs) is used. If the User has installed an APNs certificate on an iOS MDM Server, created an iOS MDM profile with a collection of settings for connection of iOS mobile devices to the Software, and installed this profile on mobile devices, the User agrees to provide the following information to APNs in automatic mode:

- Token—Push token of the device. The server uses this token when sending push notifications to the device.
- PushMagic—String that must be included in the push notification. The string value is generated by the device.

### Data transferred to AO Kaspersky Lab

If the Kaspersky Extended Detection and Response Optimum functionality is available to the User, Kaspersky Security Center Linux transfers data in the following cases:

- To assign a training course to an employee, Kaspersky Security Center Linux transfers the following data to the Kaspersky Automated Security Awareness Platform (KASAP): user email, alternate user email (if available), user ID in KASAP, training group ID.
- To automatically run a file using Kaspersky Cloud Sandbox, the managed application transfers quarantined files from the Administration Server using Network Agent, and then, using the Kaspersky Security Center Web Console, to Kaspersky Cloud Sandbox. Kaspersky Cloud Sandbox analyzes the file and any files that may be created during the execution of the file.

### Locally processed data

Kaspersky Security Center Linux is designed for centralized execution of basic administration and maintenance tasks on an organization's network. Kaspersky Security Center Linux provides the administrator with access to detailed information about the organization's network security level; Kaspersky Security Center Linux lets an administrator configure all the components of protection based on Kaspersky applications. Kaspersky Security Center Linux performs the following main functions:

- Detecting devices and their users on the organization's network
- Creating a hierarchy of administration groups for device management
- Installing Kaspersky applications on devices
- Managing the settings and tasks of installed applications
- Managing the updates for Kaspersky and third-party applications, and finding and fixing vulnerabilities
- Activating Kaspersky applications on devices
- Managing user accounts
- Viewing information about the operation of Kaspersky applications on devices
- Viewing reports
- Enabling integration with Kaspersky services

To perform its main functions Kaspersky Security Center Linux can receive, store, and process the following information:

- Information about the devices on the organization's network received through scanning of domain controllers (Active Directory, Samba, FreeIPA, and ALD Pro) or through scanning of IP intervals. Administration Server gets data independently or receives data from Network Agent.

- Information from domain controllers (Active Directory, Samba, FreeIPA and ALD Pro) about organizational units, domains, users, and groups. Administration Server gets data by itself or receives data from Network Agent assigned to work as a distribution point.

- Details of managed devices. Network Agent transfers the data listed below from the device to Administration Server. The user enters the display name and description of the device in the Kaspersky Security Center Web Console interface:

    - Technical specifications of the managed device and its components required for device identification: device display name and description, Windows domain name and type (for devices belonging to a Windows domain), device name in the Windows environment (for devices belonging to a Windows domain), DNS domain and DNS name, IPv4 address, IPv6 address, network location, MAC address, serial number, operating system type, whether the device is a virtual machine together with hypervisor type, and whether the device is a dynamic virtual machine as part of VDI.

    - Other specifications of managed devices and their components required for audit of managed devices and for making decisions about whether specific patches and updates are applicable: operating system architecture, operating system vendor, operating system build number, operating system release ID, operating system location folder, if the device is a virtual machine—the virtual machine type, name of the virtual Administration Server that manages the device.

    - Details of actions on managed devices: date and time of the last update, time the device was last visible on the network, restart waiting status, and time the device was turned on.

    - Details of device user accounts and their work sessions.

- Data received by running remote diagnostics on a managed device: trace files, system information, details of Kaspersky applications installed on the device, dump files, event logs, the results of running the diagnostic scripts received from Kaspersky Technical Support.

- Distribution point operation statistics if the device is a distribution point. Network Agent transfers data from the device to Administration Server.

- Distribution point settings entered by the User in Kaspersky Security Center Web Console.

- Data necessary for the connection of mobile devices to the Administration Server: certificate, mobile connection port, Administration Server connection address. The User enters the data in Kaspersky Security Center Web Console.

- Details of mobile devices transferred by using the mobile protocol. The data listed below is transferred from the mobile device to Administration Server:
    - Information about the application: application name, full version of the application, installation date and time of the application, real-time protection status of the device, session ID.
    - Information about the license keys used by the application: license key serial number and license type, license key status, license key validity period in days, license key generation and expiration dates, name of the company to which the license was provided, additional information in case a subscription is used (subscription flag, expiration date and number of days available for subscription renewal, web address of the subscription provider, and current subscription status and cause for obtaining this status), date and time when the application was activated on the device, date and time when the license on the device expires.
    - Information about the managed device: device name, device ID, device type, device IMEI (if available), device serial number (if available), device manufacturer, device CPU family name, device owner certificate thumbprint, OS type, OS version, OS name, total disk space on device, name of the server to which the device belongs, device IP address, device group name, distinguished name of the user, distinguished name of the domain, one-time password or domain password.
    - Information about the result of executing custom commands: command ID, command execution status, command execution result; for the device locate command: latitude, longitude, altitude, and movement speed of the device; for the mugshot command: photos taken by the front camera of the mobile device when trying to unlock.
    - Information about device scanning: date and time of the last device scan; full path in the file system from which the scan started; number of scanned object; number of detected malicious objects; number of blocked, deleted, and disinfected objects; number of objects that could not be disinfected; number of validation errors; number of terminated processes.
    - Information about the functioning of each application component and about the performance of each task, presented as events:
        - Event ID.
        - Importance level.
        - Event name and type.
        - Description of the event cause.
        - Date and time when the event occurred.
        - Information about Anti-Theft operation events (device unlock code, device coordinates, command delivery method, list of deleted data).
        - Results of processing a detected object or action (file name on the device; application name; threat name; threat type; type of action performed with the file; action result; error code, in case of occurrence).
        - Information about the triggered compliance rule (rule criterion; applied action; description of the error in applying the action, in case of occurrence).
        - Information about the application operation error (application version, OS version, device name, error description).
        - Information about the error of Samsung KNOX (error code, URL from which the file could not be downloaded).

        - Information about the permissions granted to the application.
        - Information about each of the applications installed on the managed device (application name, installation status).
        - Information about global acceptance of the End User License Agreement (EULA): EULA ID, EULA timestamp, EULA text.
        - Google Firebase Cloud Messaging Settings: Sender ID, device registration ID.
    - Information about the device's public IP address.
    - Values of user settings. The administrator manages settings in Kaspersky Security Center Web Console, while the user manages these settings in the mobile app.
- Details of mobile devices transferred by using the iOS MDM protocol. The data listed below is transferred from the mobile device to Administration Server:
    - Technical specifications of the mobile device and its components required for device identification: device name, model, operating system name, version and build number, device model number, IMEI number, phone number, UDID, MEID, serial number, amount of full and available memory, modem firmware version, Bluetooth MAC address, Wi-Fi MAC address, and SIM card details (ICCID as part of the SIM card ID).
    - Details of the mobile network used by the managed device: mobile network type, name of the currently used mobile network, name of the home mobile network, version of the mobile network operator settings, voice roaming and data roaming status, country code of the home network, residence country code, country code of the currently used network, and encryption level.
    - Security settings of the mobile device: use of a password and its compliance with the policy settings, list of installed certificates, apps and configuration profiles.
    - Date and time of last synchronization with Administration Server and device management status.
- Details of mobile device data transferred by using the WebRTC protocol: device screen image.
- Details of files specified for transfer to mobile devices. The User enters data in the Kaspersky Security Center Web Console interface.
- Details of Kaspersky applications installed on the device. The managed application transfers data from the device to Administration Server through Network Agent:
    - Settings of Kaspersky applications installed on the managed device: Kaspersky application name and version, status, real-time protection status, last device scan date and time, number of threats detected, number of objects that failed to be disinfected, availability and status of the application components, details of Kaspersky application settings and tasks, information about the active and reserve license keys, application installation date and ID.
    - Application operation statistics: events related to the changes in the status of Kaspersky application components on the managed device and to the performance of tasks initiated by the application components.
    - Device status defined by the Kaspersky application.
    - Tags assigned by the Kaspersky application.

- Data contained in events from Kaspersky Security Center Linux components and Kaspersky managed applications. Network Agent transfers data from the device to Administration Server.
- Data necessary for the integration of Kaspersky Security Center Linux with a SIEM system for event export. The User enters the data in Kaspersky Security Center Web Console.
- Data required to integrate Kaspersky Security Center Linux with domain controllers (Active Directory, Samba, FreeIPA and ALD Pro). The User enters the data in Kaspersky Security Center Web Console.
- Keytab files for connecting with Kerberos Single Sign-On (SSO). The User enters the data in Kaspersky Security Center Web Console.
- Data required to configure the connection to the proxy server for internet connection. The User enters the data in Kaspersky Security Center Web Console.
- Settings of Kaspersky Security Center Linux components and Kaspersky managed applications presented in policies and policy profiles. The User enters data in the Kaspersky Security Center Web Console interface.
- Task settings of Kaspersky Security Center Linux components and Kaspersky managed applications. The User enters data in the Kaspersky Security Center Web Console interface.
- Data processed by the Vulnerability and patch management feature. Network Agent transfers from the device to Administration Server the following information:
  - Information about the hardware detected on managed devices (Hardware registry).

    If Network Agent is installed on a device running Windows, it sends to the Administration Server the following information about the device hardware:

    - RAM
    - Mass storage devices
    - Motherboard
    - CPU
    - Network adapters
    - Monitors
    - Video adapter
    - Sound card

    If Network Agent is installed on a device running Linux or macOS, it sends to the Administration Server the following information about the device hardware, if this information is provided by the operating system:

    - Total RAM volume
    - Total volume of mass storage devices
    - Motherboard

    - CPU
    - Network adapters
  - Details of applications and patches installed on managed devices (Applications registry). The applications can be compared with the information about the executable files detected on the devices by the Application Control function.
  - Details of vulnerabilities in third-party software detected on managed devices.
  - Details of updates available for third-party applications installed on managed devices.
- Data required to download updates on isolated Administration Server to fix third-party software vulnerabilities on managed devices. The User enters and transmits data by using the Administration Server klscflag utility.
- User categories of applications The User enters data in the Kaspersky Security Center Web Console interface.
- Details of executable files detected on managed devices by the Application Control feature The managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.
- Details of files placed in Backup. The managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.
- Details of files placed in Quarantine. The managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.
- Details of files requested by Kaspersky specialists for detailed analysis The managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.
- Details of the status and triggering of Adaptive Anomaly Control rules. The managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.
- Details of external devices (memory units, information transfer tools, information hardcopy tools, and connection buses) installed or connected to the managed device and detected by the Device Control feature. The managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.
- Information about encrypted Windows devices and the encryption status. The managed application transfers data from the device to Administration Server through Network Agent.
- Information about data encryption errors on the devices. The encryption is performed by the Encryption data function of Kaspersky applications. The managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.
- List of managed programmable logic controllers (PLCs) The managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.
- Data required for creation of a threat development chain. The managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.

- Information about attempts by an organization's employees to access cloud services. The managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.

- Data required for Kaspersky Security Center integration with the Kaspersky Managed Detection and Response service (the dedicated plug-in must be installed for Kaspersky Security Center Web Console): integration initiation token, integration token, and user session token. The User enters the integration initiation token in the Kaspersky Security Center Web Console interface. The Kaspersky MDR service transfers the integration token and the user session token through the dedicated plug-in.

- Data required to integrate Kaspersky Security Center Linux with Kaspersky Cloud Sandbox and Kaspersky Threat Intelligence Portal (requires installation of the appropriate plug-in for Kaspersky Security Center Web Console): an integration token, an authorization token. The User enters a token for integration in the Kaspersky Security Center Web Console interface. Kaspersky Security Center Web Console transfers an authorization token in a request to the Kaspersky Cloud Sandbox API.

- Data required to integrate Kaspersky Security Center Linux with the Kaspersky Automated Security Awareness Platform (KASAP) service: API token for accessing the KASAP Open API, URL (a link for accessing KASAP through Open API).

- Details of the entered activation codes and key files. The User enters data in the Kaspersky Security Center Web Console interface.

- User accounts: name, description, full name, email address, main phone number, password, secret key generated by Administration Server, and one-time password for two-factor authentication. The User enters data in the Kaspersky Security Center Web Console interface.

- Revision history of management objects The User enters data in the Kaspersky Security Center Web Console interface.

- IP address of the device on which a user created a revision. The IP address is defined by Administration Server automatically.

- Registry of deleted management objects. The User enters data in the Kaspersky Security Center Web Console interface.

- Installation packages created from the file, as well as installation settings. The User enters data in the Kaspersky Security Center Web Console interface.

- Data required for the display of announcements from Kaspersky in Kaspersky Security Center Web Console. The User enters data in the Kaspersky Security Center Web Console interface.

- Data required for the functioning of plug-ins of managed applications in Kaspersky Security Center Web Console and saved by the plug-ins in the Administration Server database during their routine operation. The description and ways of providing the data are provided in the Help files of the corresponding application.

- Kaspersky Security Center Web Console user settings: localization language and theme of the interface, Monitoring panel display settings, information about the status of notifications (Already read / Not yet read), status of columns in spreadsheets (Show / Hide), Training mode progress. The User enters data in the Kaspersky Security Center Web Console interface.

- Certificate for secure connection of managed devices to the Kaspersky Security Center Linux components. The User enters and transmits data by using the Administration Server klsetsrvcert utility.

- Certificates for establishing trust to the internal web resources of the organization. The User enters data in the Kaspersky Security Center Web Console interface.

- Information about the user accepting the terms and conditions of legal agreements with Kaspersky.
- The Administration Server data that the User enters in the Kaspersky Security Center Web Console or program interface Kaspersky Security Center OpenAPI.
- Any data that the User enters in the Kaspersky Security Center Web Console interface.

The data listed above can be present in Kaspersky Security Center Linux if one of the following methods is applied:

- The User enters data in the Kaspersky Security Center Web Console interface.
- Network Agent automatically receives data from the device and transfers it to Administration Server.
- Network Agent receives data retrieved by the Kaspersky managed application and transfers it to Administration Server. The lists of data processed by Kaspersky managed applications are provided in the Help files for the corresponding applications.
- Administration Server gets the information about the networked devices by itself or receives data from Network Agent assigned to work as a distribution point.
- Data is transferred from the mobile device to Administration Server by using the iOS MDM protocol or mobile protocol.

The listed data is stored in the Administration Server database. Password hashes are stored in encrypted form.

All data processed locally can be transferred to Kaspersky only through dump files, trace files, or log files of Kaspersky Security Center Linux components, including log files created by installers and utilities.

The dump files, trace files, or log files of Kaspersky Security Center Linux components contain arbitrary data of Administration Server, Network Agent, and Kaspersky Security Center Web Console. The files may contain personal or confidential data. The dump files, trace files, or log files are stored on the devices in an unencrypted form. The dump files, trace files, or log files are not transferred to Kaspersky automatically, but an administrator may transfer those files to Kaspersky manually by request from Technical Support to resolve issues related to Kaspersky Security Center Linux performance.

The obtained information is protected by Kaspersky Lab in accordance with the requirements established by law and the current rules of Kaspersky Lab. Data is transmitted over secure communication channels.

Following the links in Kaspersky Security Center Web Console, the User agrees to the automatic transfer of the following data:

- Kaspersky Security Center Linux code
- Kaspersky Security Center Linux version
- Kaspersky Security Center Linux localization
- License ID
- License type
- Whether the license was purchased through a partner

The list of data provided via each link depends on the purpose and location of the link.

Kaspersky uses the collected data in anonymized form and only for general statistical purposes. Summary statistics is generated from the received raw data automatically and does not contain any personal or other confidential information. When new data accumulates, older data is erased (once a year). Summary statistics is stored indefinitely.

# About the subscription

*Subscription to Kaspersky Security Center Linux* is an order for use of the application under the selected settings (subscription expiration date, number of protected devices). You can register your subscription to Kaspersky Security Center Linux with your service provider (for example, your internet provider). A subscription can be renewed manually or in automatic mode; also, you can cancel it.

A subscription can be limited (for example, one-year) or unlimited (with no expiration date). To continue using Kaspersky Security Center after a limited subscription expires, you must renew it. An unlimited subscription is renewed automatically if it has been prepaid to the service provider in due dates.

When a limited subscription expires, you may be provided a grace period for renewal during which the application continues to function. The availability and duration of the grace period is defined by the service provider.

To use Kaspersky Security Center Linux under subscription, you must apply the activation code received from the service provider.

You can apply a different activation code for Kaspersky Security Center Linux only after your subscription expires or when you cancel it.

Depending on the service provider, the set of possible actions for subscription management may vary. The service provider might not provide a grace period for subscription renewal and so the application loses its functionality.

Activation codes purchased under subscription cannot be used for activating earlier versions of Kaspersky Security Center.

When the application is used under subscription, Kaspersky Security Center Linux automatically attempts to access the activation server at specified time intervals until the subscription expires. If access to the server using system DNS is not possible, the application uses public DNS servers. You can renew your subscription on the service provider's website.

# Activating Kaspersky Security Center Linux

You can activate Kaspersky Security Center Linux to use its additional functionality. There are two ways to accomplish this task: use the Administration Server Quick Start Wizard or the Administration Server properties.

*To activate Kaspersky Security Center Linux:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **License keys** section.

3. Under **Current license**, click the **Select** button.

4. In the window that opens, select the license key that you want to use to activate Kaspersky Security Center Linux. If the license key is not listed, click the **Add new license key** button, and then specify a new license key.

5. If necessary, you can also add a reserve license key. To do this, under **Reserve license key**, click the **Select** button, and then select an existing license key or add a new one. Note that you cannot add a reserve license key if there is no active license key.

6. Click the **Save** button.

# Licensing of managed Kaspersky applications

This section describes the features of Kaspersky Security Center related to working with the license keys of managed Kaspersky applications.

Kaspersky Security Center Linux allows you to perform centralized distribution of license keys for Kaspersky applications on client devices, monitor their use, and renew licenses.

When adding a license key using Kaspersky Security Center, the settings of the license key are saved on the Administration Server. Based on this information, the application generates a license key usage report and notifies the administrator of license expirations and violation of license restrictions that are set in the properties of license keys. You can configure notifications of the use of license keys within the Administration Server settings.

## Licensing of managed applications

The Kaspersky applications installed on managed devices must be licensed by applying a key file or activation code to each of the applications. A key file or activation code can be deployed in the following ways:

- Automatic deployment
- The installation package of a managed application
- The Add license key task for a managed application
- Manual activation of a managed application

You can add a new active or reserve license key by any of the methods listed above. A Kaspersky application uses an active key at the current moment and stores a reserve key to apply after the active key expires. The application for which you add a license key defines whether the key is active or reserve. The key definition does not depend on the method that you use to add a new license key.

### Automatic deployment

If you use different managed applications and you have to deploy a specific key file or activation code to devices, opt for other ways of deploying that activation code or key file.

Kaspersky Security Center allows you to automatically deploy available license keys to devices. For example, three license keys are stored in the Administration Server repository. You have enabled the **Automatically distributed license key** option for all three license keys. A Kaspersky security application—for example, Kaspersky Endpoint Security for Linux—is installed on the organization's devices. A new device is discovered to which a license key must be deployed. The application determines, for instance, that two of the license keys from the repository can be applied to the device: license key named *Key_1* and license key named *Key_2*. One of these license keys is deployed to the device. In this case, it cannot be predicted which of the two license keys will be deployed to the device because automatic deployment of license keys does not provide for any administrator activity.

When a license key is deployed, the devices are recounted for that license key. You must make sure that the number of devices to which the license key was deployed does not exceed the license limit. If the number of devices exceeds the license limit, all devices that were not covered by the license will be assigned *Critical* status.

Before deployment, the key file or activation code must be added to the Administration Server repository.

How-to instructions:

- Adding a license key to the Administration Server repository
- Automatic distribution of a license key

Note that an automatically distributed license key may not be displayed in the virtual Administration Server repository in the following cases:

- The license key is not valid for the application.
- The virtual Administration Server does not have managed devices.
- The license key has already been used for devices managed by another virtual Administration Server and the limit on the number of devices has been reached.

### Adding a key file or activation code to the installation package of a managed application

For security reasons, this option is not recommended. A key file or activation code added to an installation package may be compromised.

If you install a managed application using an installation package, you can specify an activation code or key file in this installation package or in the policy of the application. The license key will be deployed to managed devices at the next synchronization of the device with the Administration Server.

How-to instructions: Adding a license key to an installation package

### Deployment through the Add license key task for a managed application

If you opt to use the Add license key task for a managed application, you can select the license key that must be deployed to devices, and then select the devices in any convenient way—for example, by selecting an administration group or a device selection.

Before deployment, the key file or activation code must be added to the Administration Server repository.

How-to instructions:

- Adding a license key to the Administration Server repository
- Deploying a license key to client devices

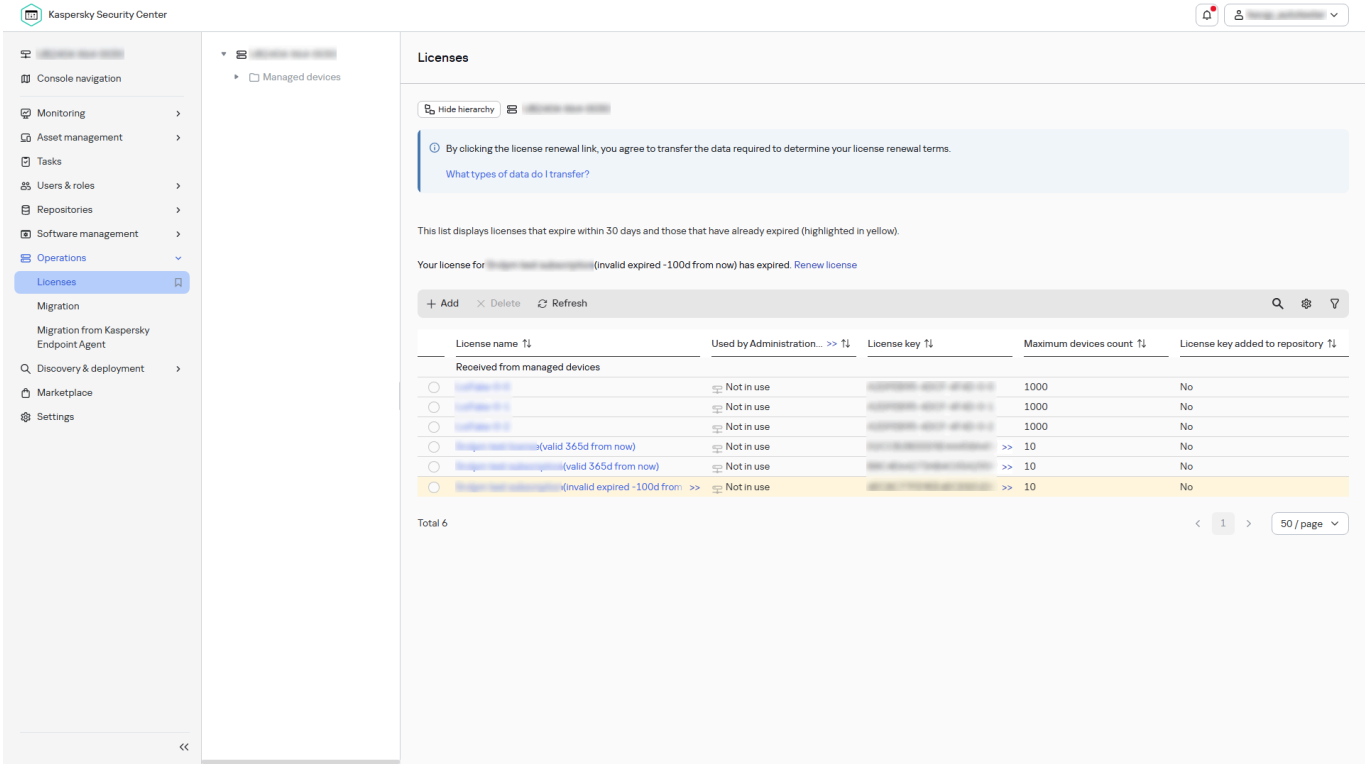
Adding an activation code or a key file manually to the devices

You can activate the installed Kaspersky application locally, by using the tools provided in the application interface. Please refer to the documentation of the installed application.

# Adding a license key to the Administration Server repository

*To add a license key to the Administration Server repository:*

1. In the main menu, go to **Operations** → **Licenses**.



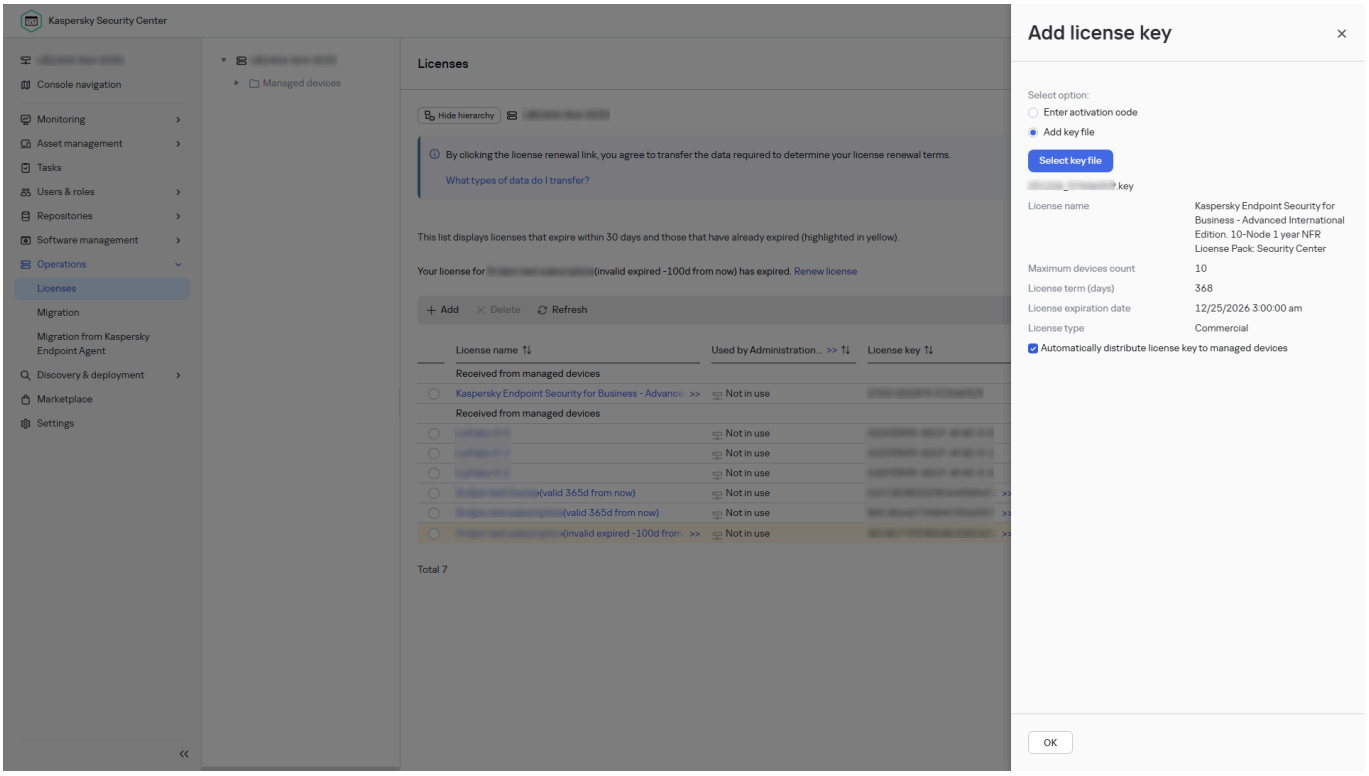

List of added Kaspersky license keys

2. Click **Add**.

3. Choose what you want to add:

- **Add key file**

  Click the **Select key file** button and browse to the .key file that you want to add.




Adding a license key by applying a key file

- **Enter activation code**

  Specify the activation code in the text field and click the **Send** button.

4. Click the **Close** button.

The license key or several license keys are added to the Administration Server repository.

# Deploying a license key to client devices

Kaspersky Security Center Web Console allows you to distribute a license key to client devices automatically or through the **Application activation** task. You can use the task to distribute keys to a specific device group. During distribution of a license key via the task, the licensing limit on the number of devices is not taken into account. Use the automatic key distribution to cease distribution of a license key automatically when the licensing limit is reached.

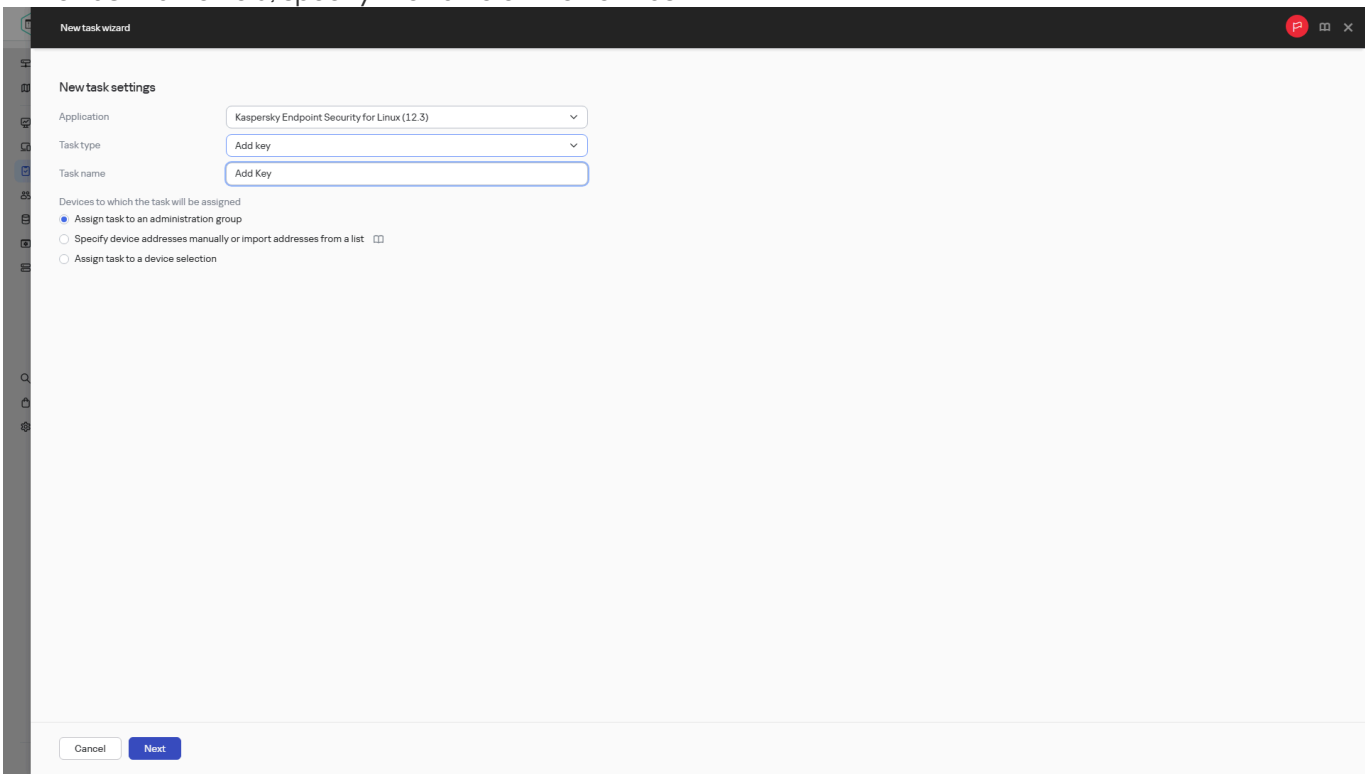
If you enable automatic distribution of a license key, do not create an **Application activation** task to distribute that key to client devices. Otherwise, the load on the Administration Server will increase due to frequent synchronization.

Before deployment, add the license key to the Administration Server repository.

*To distribute a license key to client devices through the **Application activation** task:*

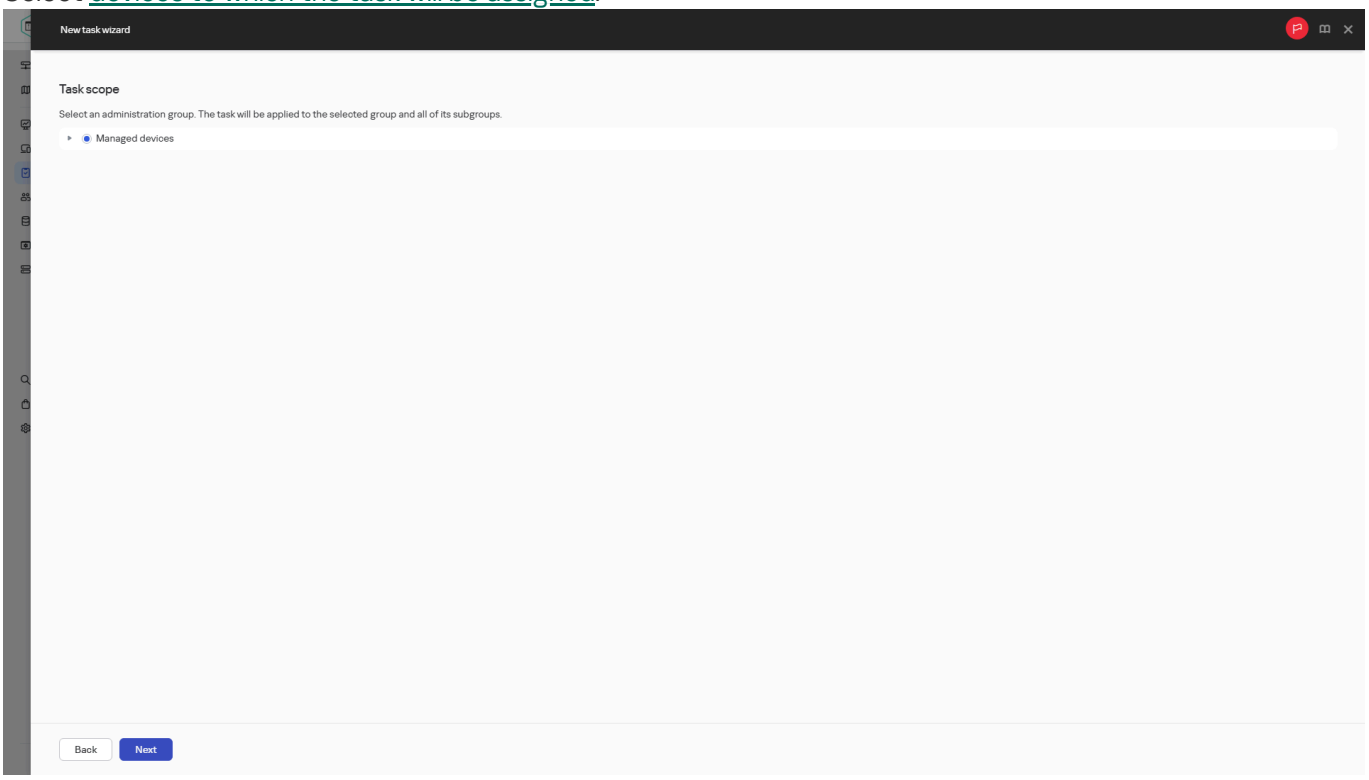
1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The **New task wizard** starts. Proceed through the wizard by using the **Next** button.
3. In the **Application** drop-down list, select the application for which you want to add a license key.
4. In the **Task type** list, select the **Application activation** task.
5. In the **Task name** field, specify the name of the new task.




Creating an Add Key task

6. Select devices to which the task will be assigned.




Specifying the task scope

7. At the **Selecting a license key** step of the wizard, click the **Add key** link to add the license key.

8. On the key adding pane, add the license key by using one of the following options:

> You need to add the license key only if you did not add it to the Administration Server repository prior to creating the **Application activation** task.

- Select the **Enter activation code** option to enter an activation code, and then do the following:

  a. Specify the activation code, and then click the **Send** button.

  Information about the license key appears in the key adding pane.

  b. Click the **Save** button.

  > If you want to distribute the license key to managed devices automatically, enable the **Automatically distribute license key to managed devices** option.

  The key adding pane closes.

- Select the **Add key file** option to add a key file, and then do the following:

  a. Click the **Select key file** button.

  b. In the window that opens, select a key file, and then click the **Open** button.

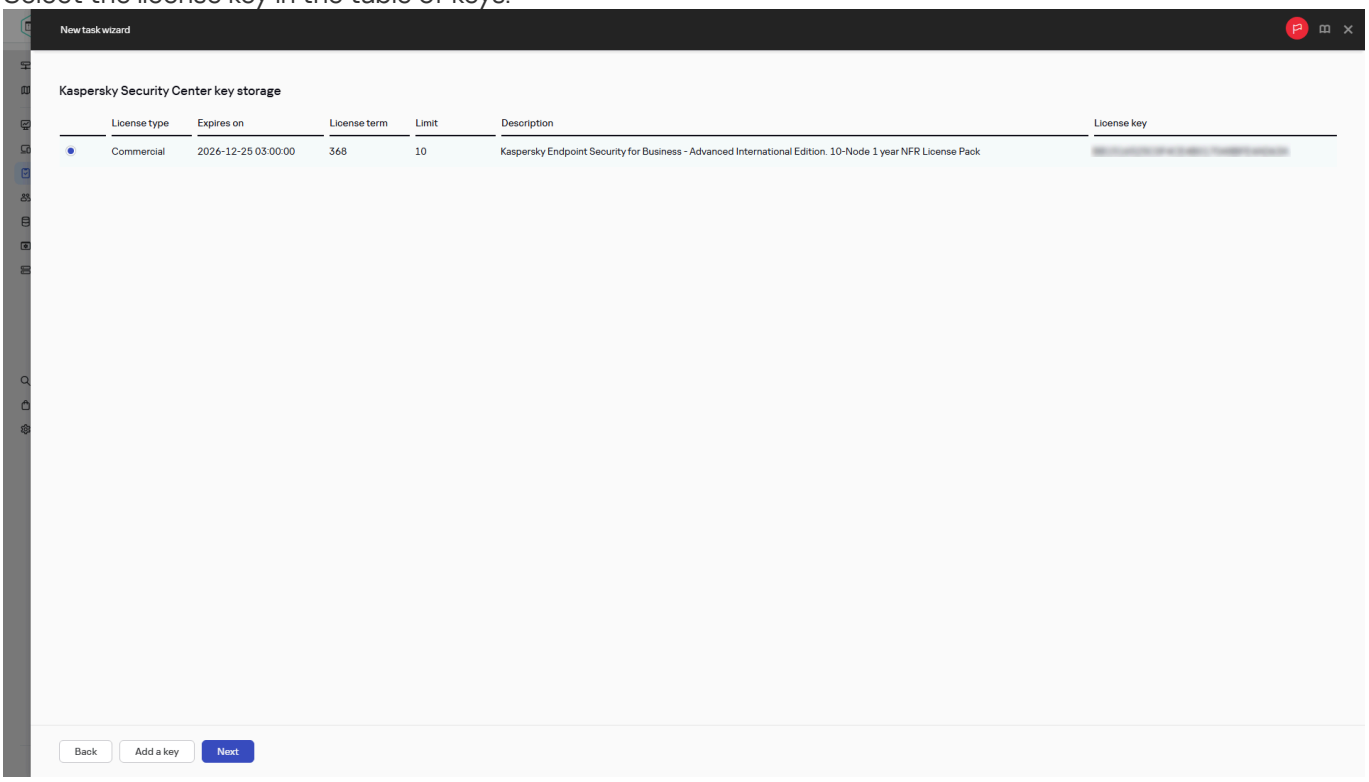
  Information about the license key appears in the license key adding pane.

  c. Click the **Save** button.

If you want to distribute the license key to managed devices automatically, enable the **Automatically distribute license key to managed devices** option.

The key adding pane closes.

9. Select the license key in the table of keys.

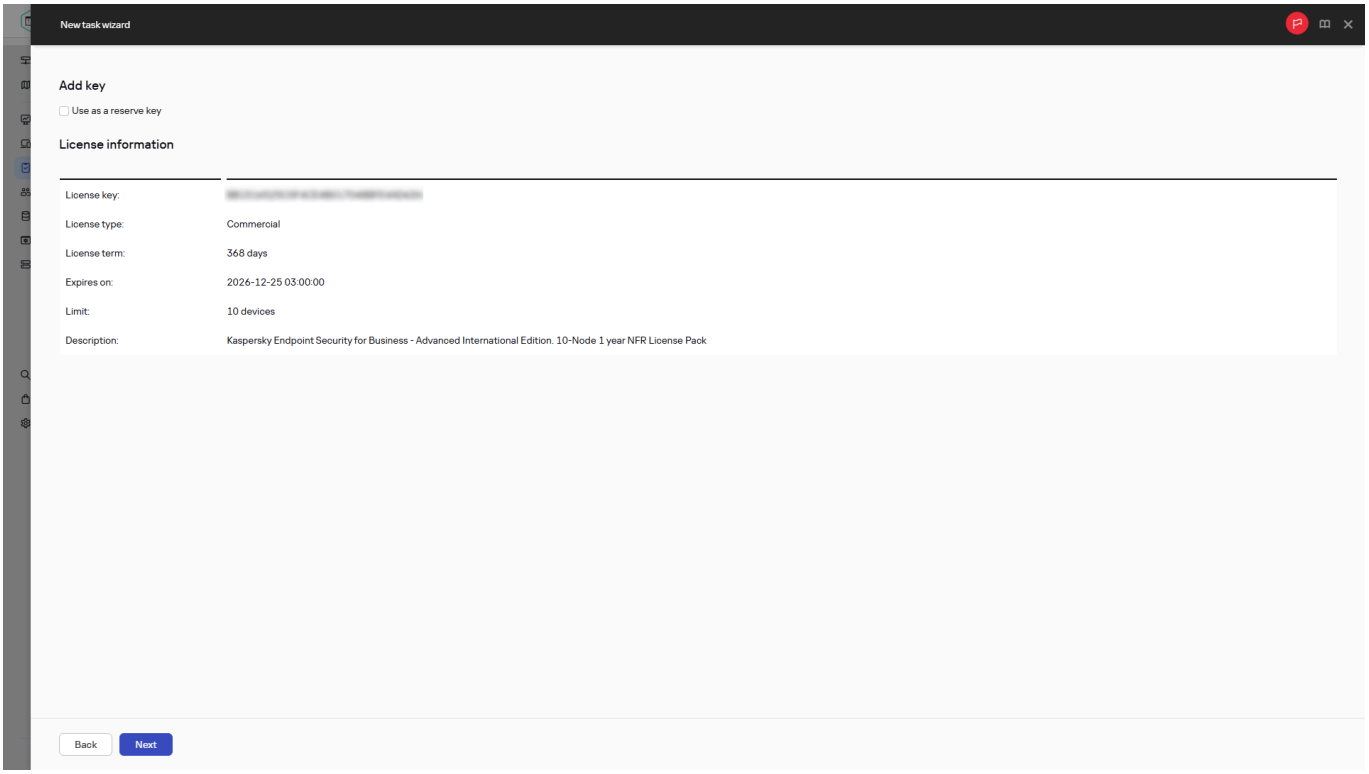



Selecting the license key

10. At the **License information** step of the wizard, clear the default **Use as a reserve key** check box if you want to replace the active license key.

    For example, this is needed when the organization changes, and another organization's key is required on the device; or if the key was reissued, and a new license expires earlier than the current license. To avoid errors, you have to clear the **Use as a reserve key** check box.

If you want to find out more information about the issues that may occur when adding a license key to Kaspersky Security Center and the ways to resolve them, refer to the Kaspersky Security Center Knowledge Base.




Specifying the reserve license key

11. At the **Finish task creation** step of the wizard, enable the **Open task details when creation is complete** option to modify the default task settings.

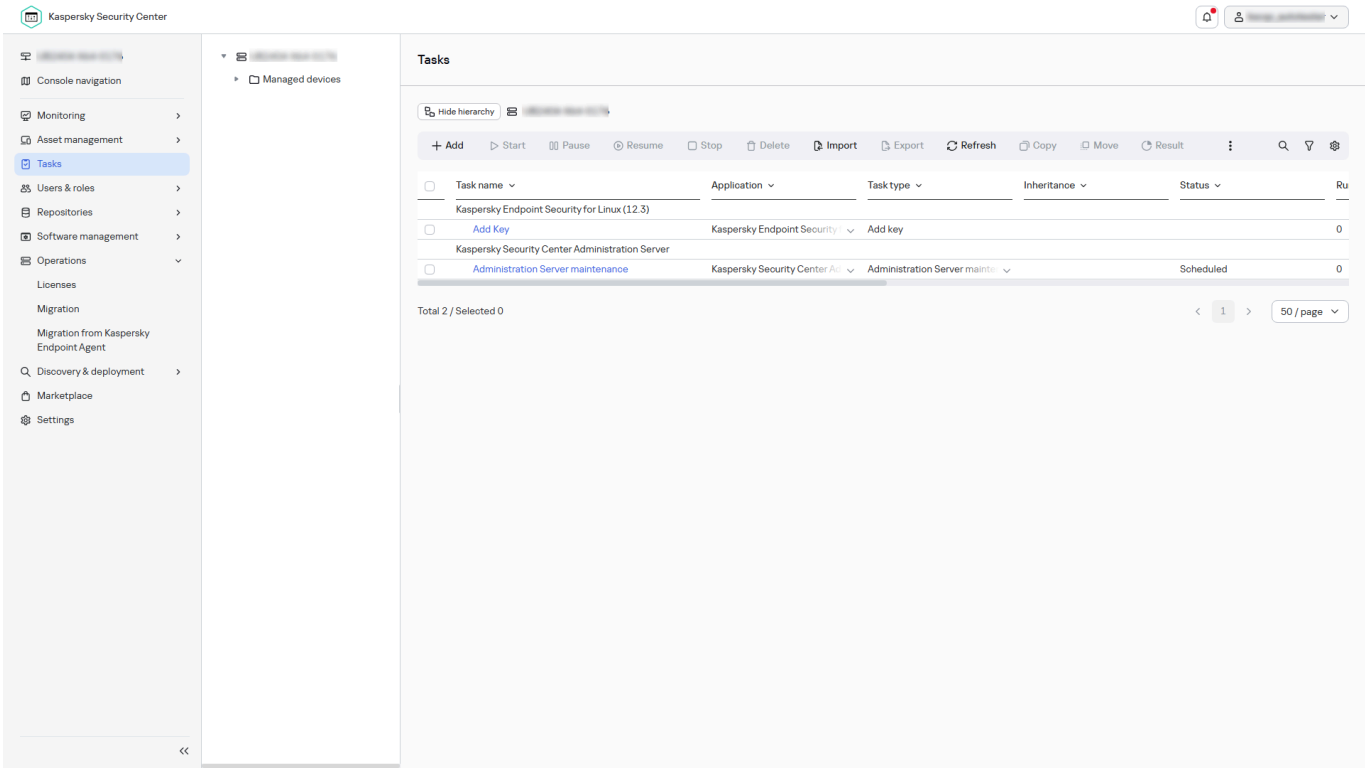
    If you do not enable this option, the task is created with the default settings. You can modify the default settings later.

12. Click the **Finish** button.

    The wizard creates the task. If you enabled the **Open task details when creation is complete** option, the task properties window automatically opens. In this window, you can specify the general task settings and, if required, change the settings specified during task creation.

    You can also open the task properties window by clicking the name of the created task in the list of tasks.

The task is created, configured, and displayed in the list of tasks.




The task list

13. To run the task, select it in the task list, and then click the **Start** button.

    You can also set a task start schedule on the **Schedule** tab of the task properties window.

    For a detailed description of scheduled start settings, refer to the general task settings.

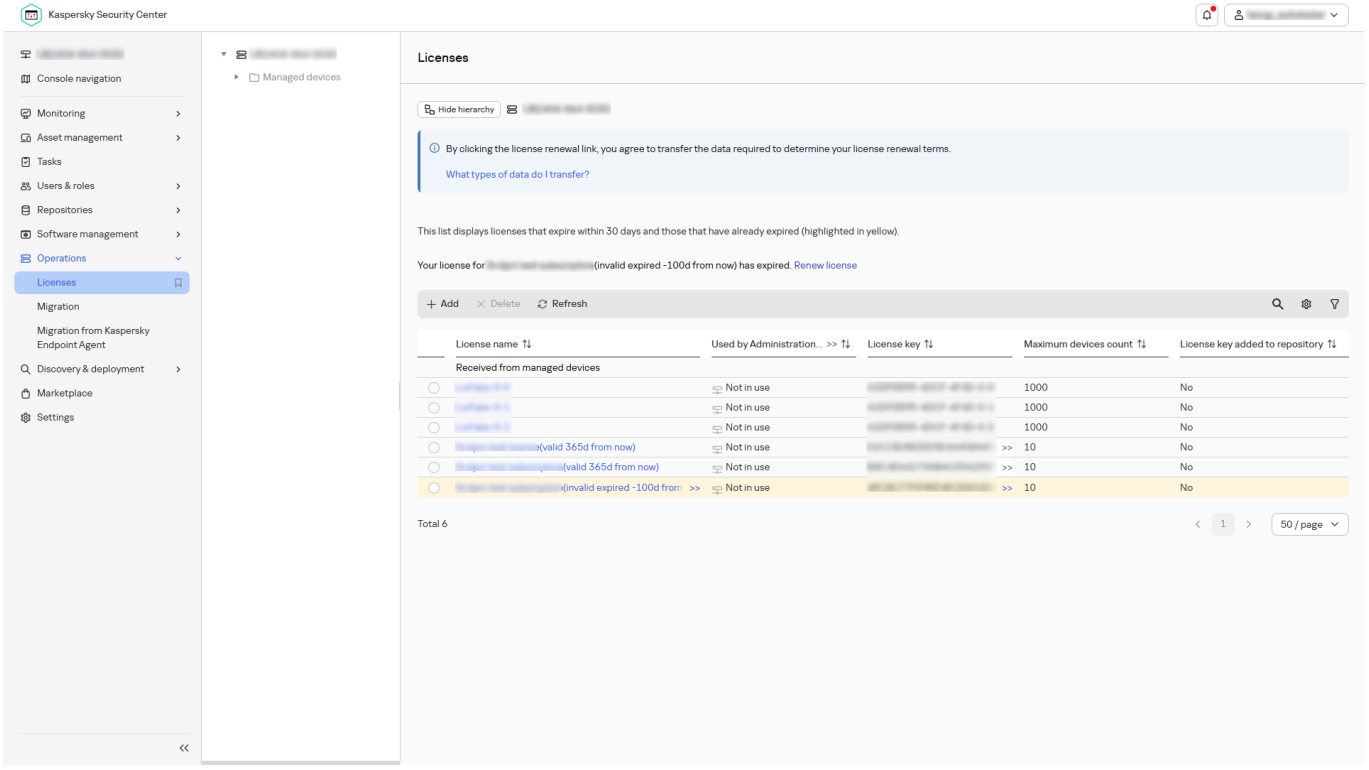
After the task is completed, the license key is deployed to the selected devices.

# Automatic distribution of a license key

Kaspersky Security Center Linux allows automatic distribution of license keys to managed devices if they are located in the license keys repository on the Administration Server.

*To distribute a license key to managed devices automatically:*

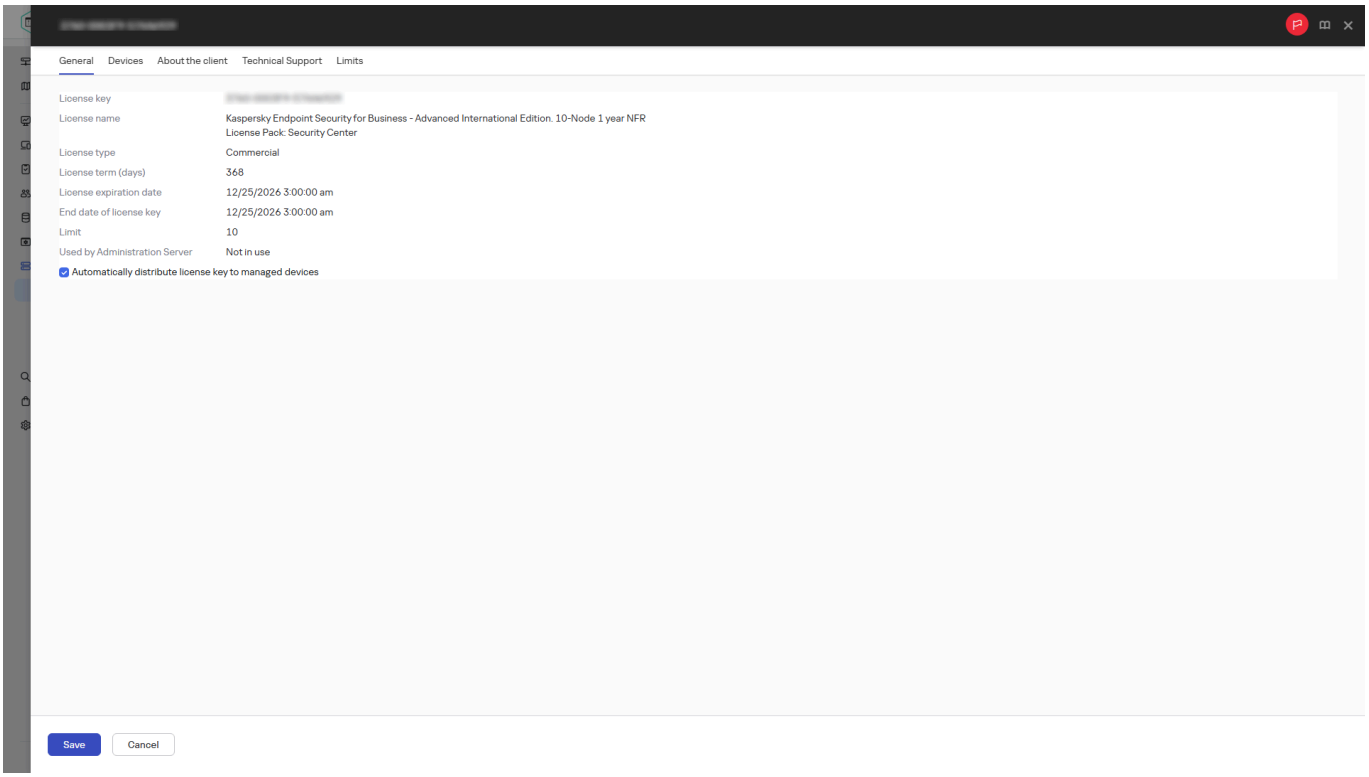
1. In the main menu, go to **Operations → Licensing → Licenses**.




The license list

2. Click the name of the license key that you want to distribute to devices automatically.

3. In the license key properties window that opens, select the **Automatically distribute license key to managed devices** check box.




The license key properties window

4. Click the **Save** button.

The license key will be automatically distributed to all compatible devices.

License key distribution is performed by means of Network Agent. No license key distribution tasks are created for the application.

During automatic distribution of a license key, the licensing limit on the number of devices is taken into account. The license limit is set in the properties of the license key. If the license limit is reached, distribution of this license key on devices ceases automatically.

Note that an automatically distributed license key may not be displayed in the virtual Administration Server repository in the following cases:

- The license key is not valid for the application.
- The virtual Administration Server does not have managed devices.
- The license key has already been used for devices managed by another virtual Administration Server and the limit on the number of devices has been reached.

The virtual Administration Server automatically distributes license keys from its repository and from the repository of the Administration Server. We recommend that you:

- Use the *Add license key* task to select the license key that must be deployed to devices.
- Avoid disabling the **Allow automatic deployment of license keys from this virtual Administration Server to its devices** option in the virtual Administration Server settings. Otherwise, the virtual Administration Server will not distribute license keys to devices, including the license keys from the Administration Server repository.

If you select the **Automatically distribute license key to managed devices** check box in the license key properties window, a license key is distributed on your network immediately. If you do not select this option, you can use a task to distribute a license key later.

Automatic distribution of license keys configured on the primary Administration Server does not extend to devices managed by non-virtual secondary Administration Servers.

# Viewing information about license keys in use

*To view the list of the license keys added to the Administration Server repository:*

In the main menu, go to **Operations** → **Licensing** → **Licenses**.

The displayed list contains the key files and activation codes added to the Administration Server repository.

*To view detailed information about a license key:*

1. In the main menu, go to **Operations** → **Licensing** → **Licenses**.
2. Click the name of the required license key.

In the license key properties window that opens, you can view:

- On the **General** tab—The main information about the license key
- On the **Devices** tab—The list of client devices where the license key was used for activation of the installed Kaspersky application
- On the **Limits** tab—The list of license limits

  If you activated Administration Server under Kaspersky Next XDR Optimum license, the **Limits** tab displays the **XDR-O** field with the **Enabled** value.

*To view which license keys are deployed to a specific client device:*

1. In the main menu, go to **Asset management** → **Managed devices**.
2. Click the name of the required device.
3. In the device properties window that opens, select the **Applications** tab.
4. Click the name of the application for which you want to view the information about the license key.
5. In the application properties window that opens, select the **General** tab, and then open the **License** section.

The main information about the active and reserve license keys is displayed.

To define the up-to-date settings of virtual Administration Server license keys, the Administration Server sends a request to Kaspersky activation servers at least once per day. If access to the servers using system DNS is not possible, the application uses public DNS servers.

# Events of the license limit exceeded

Kaspersky Security Center Linux allows you to get information about events when some license limits are exceeded by Kaspersky applications installed on client devices.

The importance level of such events when a license limit is exceeded is defined according to the following rules:

- If the currently used units covered by a single license constitute 90–100% of the total number of units covered by the license, the event is published with the **Info** importance level.
- If the currently used units covered by a single license constitute 100–110% of the total number of units covered by the license, the event is published with the **Warning** importance level.
- If the number of currently used units covered by a single license exceeds 110% of the total number of units covered by the license, the event is published with the **Critical event** importance level.

# Deleting a license key from the repository

When you delete the active license key deployed to a managed device, the application will continue working on the managed device.

*To delete a key file or activation code from the Administration Server repository:*

1. Check that Administration Server does not use a key file or activation code that you want to delete. If the Administration Server does, you cannot remove the key. To run the test:

   a. In the main menu, click the Administration Server name.

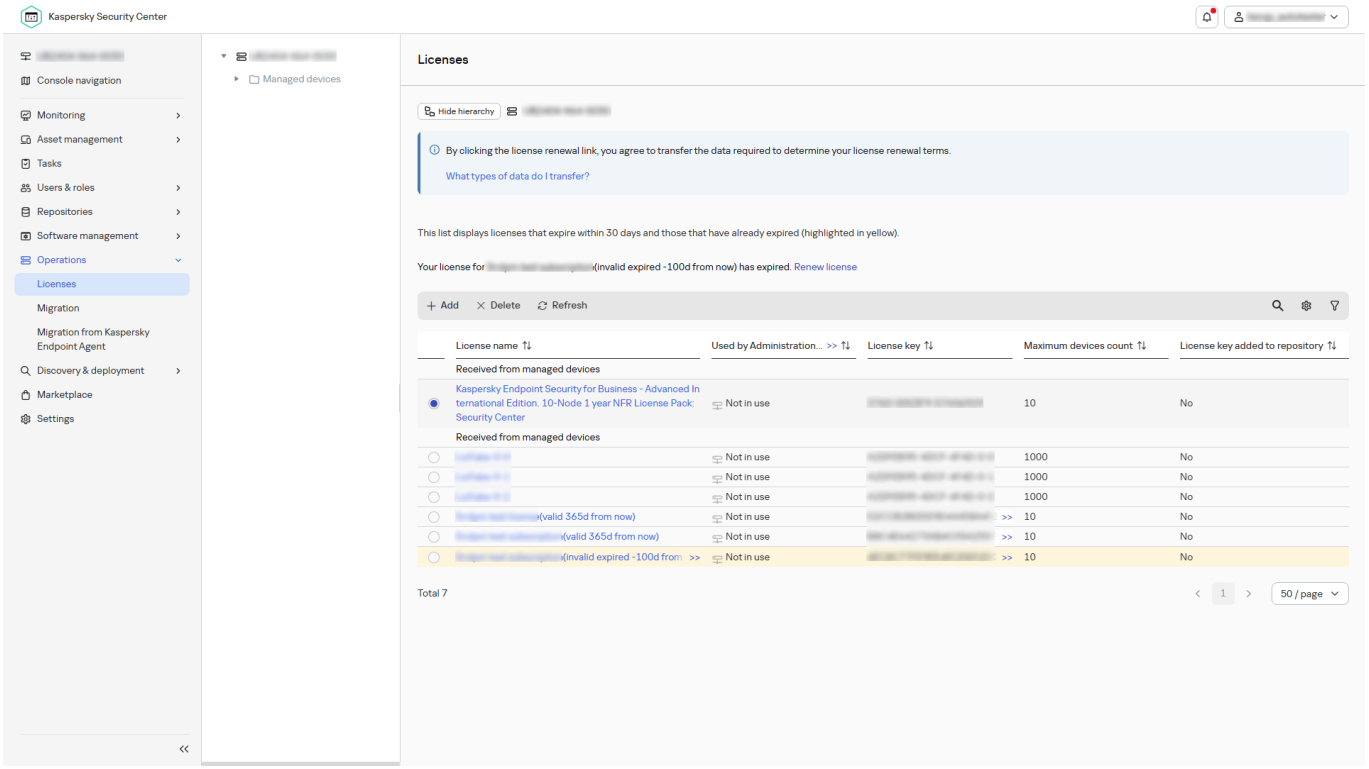
      The Administration Server properties window opens.

   b. On the **General** tab, select the **License keys** section.

   c. If the required key file or activation code is displayed in the section that opens, click the **Remove active license key** button, and then confirm the operation. After that, the Administration Server does not use the removed license key, but the key remains in the Administration Server repository. If the required key file or activation code is not displayed, the Administration Server does not use it.

2. In the main menu, go to **Operations** → **Licensing** → **Licenses**.

3. Select the required key file or activation code, and then click the **Delete** button.




The license list

The selected key file or activation code is deleted from the repository.

You can add a removed license key again or add a new one.

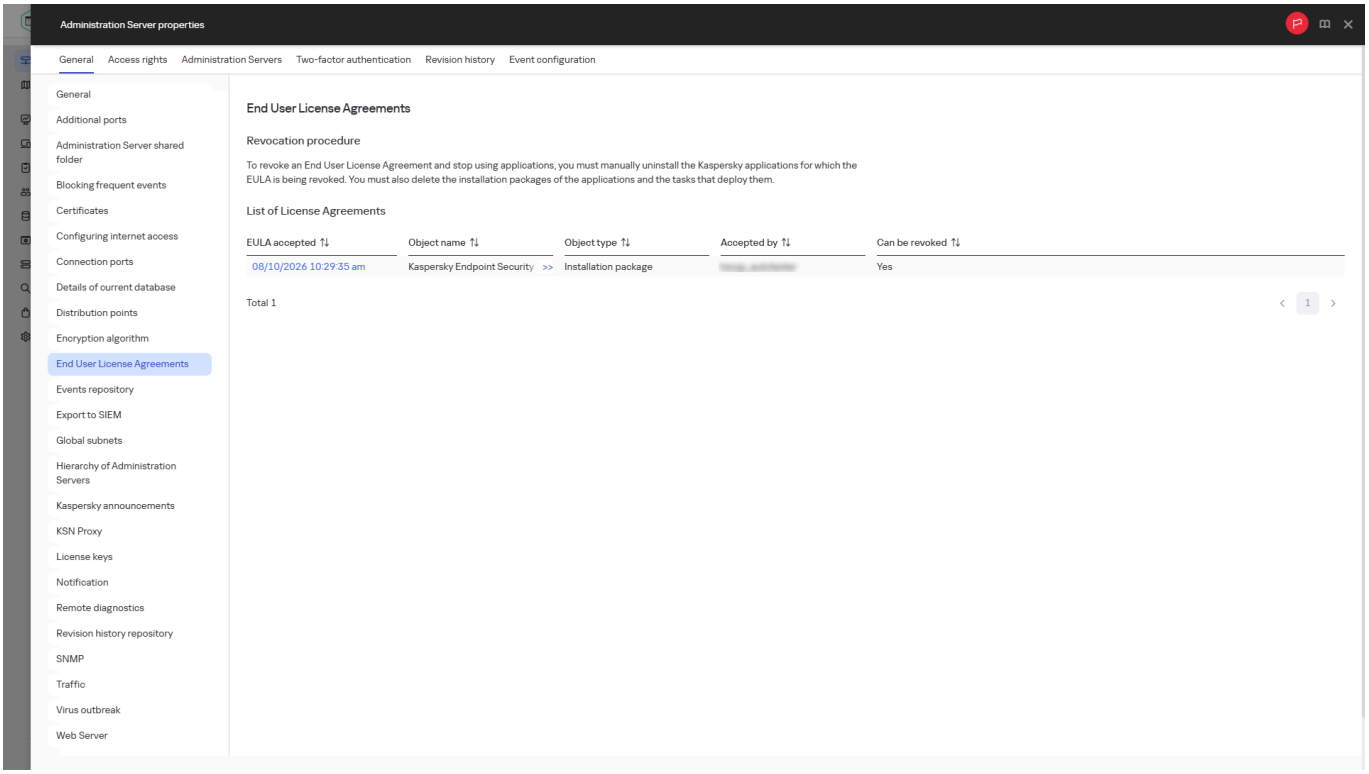
# Revoking consent with an End User License Agreement

If you decide to stop protecting some of your client devices, you can revoke the End User License Agreement (EULA) for any managed Kaspersky application. You must uninstall the selected application before revoking its EULA.

*To revoke a EULA for managed Kaspersky applications:*

1. Open the Administration Server properties window and on the **General** tab, select the **End User License Agreements** section.

A list of EULAs—accepted upon creation of installation packages, at the seamless installation of updates, or upon deployment of Kaspersky Security for Mobile—is displayed.




The list of EULAs

2. In the list, select the EULA that you want to revoke.

   You can view the following properties of the EULA:

   - Date when the EULA was accepted
   - Name of the user who accepted the EULA

3. Click the acceptance date of any EULA to open its properties window that displays the following data:

   - Name of the user who accepted the EULA
   - Date when the EULA was accepted
   - Unique identifier (UID) of the EULA
   - Full text of the EULA
   - List of objects (installation packages, seamless updates, mobile apps) linked to the EULA, and their respective names and types

4. In the lower part of the EULA properties window, click the **Revoke License Agreement** button.

   If there exist any objects (installation packages and their respective tasks) that prevent the EULA from being revoked, the corresponding notification is displayed. You cannot proceed with revocation until you delete these objects.

In the window that opens, you are informed that you must first uninstall the Kaspersky application corresponding to the EULA.

5. Click the button to confirm revocation.

The EULA is revoked. It is no longer displayed in the list of License Agreements in the **End User License Agreements** section. The EULA properties window closes; the application is no longer installed.

# Renewing licenses for Kaspersky applications

You can renew a Kaspersky application license that has expired or is about to expire (in less than 30 days).

*To renew an expired license or a license that is about to expire:*

1. Do one of the following:

   - In the main menu, go to **Operations** → **Licensing** → **Licenses**.
   - In the main menu, go to **Monitoring** → **Dashboard**, and then click the **View expiring licenses** link next to a notification.

   The **Licenses** window opens, where you can view and renew licenses.

2. Click the **Renew license** link next to the required license.

   By clicking a license renewal link, you agree to transfer to Kaspersky the following information about Kaspersky Security Center Linux: its version, the localization you are using, the software license ID (that is, the ID of the license you are renewing), and whether you purchased the license via a partner company or not.

3. In the window of the license renewal service that opens follow the instructions to renew a license.

   The license is renewed.

In Kaspersky Security Center Web Console, the notifications are displayed when a license is about to expire, according to the following schedule:

- 30 days before the expiration
- 7 days before the expiration
- 3 days before the expiration
- 24 hours before the expiration
- When a license has expired

# Using Kaspersky Marketplace to choose Kaspersky business solutions

**Marketplace** is a section in the main menu that enables you to view the entire range of Kaspersky business solutions, select the ones you need, and proceed to the purchase at the Kaspersky website. You can use filters to view only those solutions that fit your organization and the requirements for your information security system. When you select a solution, Kaspersky Security Center Linux redirects you to the related webpage at the Kaspersky website to learn more about that solution. Each webpage enables you to proceed to the purchase or contains instructions on the purchase process.

In the **Marketplace** section, you can filter Kaspersky solutions by using the following criteria:

- Number of devices (endpoints, servers, and other types of assets) that you want to protect:
  - 50–250
  - 250–1000
  - More than 1000
- Maturity level of your organization's information security team:
  - **Foundations**

    This level is typical for enterprises that only have an IT team. The maximum possible number of threats is blocked automatically.
  - **Optimum**

    This level is typical for enterprises that have a specific IT security function within the IT team. At this level, companies require solutions that enable them to counter commodity threats and threats that circumvent existing preventive mechanisms.
  - **Expert**

    This level is typical for enterprises with complex and distributed IT environments. The IT security team is mature or the company has an SOC (Security Operations Center) team. The required solutions enable the companies to counter complex threats and targeted attacks.
- Types of assets that you want to protect:
  - **Endpoints**: workstations of employees, physical and virtual machines, embedded systems
  - **Servers**: physical and virtual servers
  - **Cloud**: public, private, or hybrid cloud environments; cloud services
  - **Network**: local area network, IT infrastructure
  - **Service**: security-related services provided by Kaspersky

*To find and purchase a Kaspersky business solution:*

1. In the main menu, go to **Marketplace**.

   By default, the section displays all available Kaspersky business solutions.

2. To view only those solutions that suit your organization, select the required values in the filters.

3. Click the solution that you want to purchase or you want to learn more about.

You will be redirected to the solution webpage. You can follow the on-screen instructions to proceed to the purchase.

# Configuring Kaspersky applications

This section contains information about manual configuration of policies and tasks, about user roles, about building an administration group structure and hierarchy of tasks.

# Scenario: Configuring network protection

The quick start wizard creates policies and tasks with the default settings. These settings may turn out to be sub-optimal or even disallowed by an organization. Therefore, we recommend that you fine-tune these policies and tasks, and then create other policies and tasks if they are necessary for your network.

## Prerequisites

Before you start, make sure that you have done the following:

- Installed Kaspersky Security Center Linux Administration Server
- Installed Kaspersky Security Center Web Console
- Completed the Kaspersky Security Center Linux main installation scenario
- Completed the quick start wizard or manually created the following policies and tasks in the **Managed devices** administration group:
  - Policy of Kaspersky Endpoint Security
  - Group task for updating Kaspersky Endpoint Security
  - Policy of Network Agent
  - *Find vulnerabilities and required updates* task

## Stages

Configuring network protection proceeds in stages:

1. **Setup and propagation of Kaspersky application policies and policy profiles**

   To configure and propagate settings for Kaspersky applications installed on the managed devices, you can use two different security management approaches—device-centric or user-centric. These two approaches can also be combined.

2. **Configuring tasks for remote management of Kaspersky applications**

   Check the tasks created with the quick start wizard and fine-tune them, if necessary.

How-to instructions: Setting up the group task for updating Kaspersky Endpoint Security, Creating the Find vulnerabilities and required updates task.

If necessary, create additional tasks to manage the Kaspersky applications installed on the client devices.

3. **Evaluating and limiting the event load on the database**

   Information about events that occur during operation of managed applications is transferred from a client device and registered in the Administration Server database. To reduce the load on the Administration Server, evaluate and limit the maximum number of events that can be stored in the database.

   How-to instructions: Setting the maximum number of events.

Results

Upon completion of this scenario, your network will be protected by configuration of Kaspersky applications, tasks, and events received by the Administration Server:

- The Kaspersky applications are configured according to the policies and policy profiles.
- The applications are managed through a set of tasks.
- The maximum number of events that can be stored in the database is set.

When the network protection configuration is complete, you can proceed to configuring regular updates to Kaspersky databases and applications.

# About device-centric and user-centric security management approaches

You can manage security settings from the standpoint of device features and from the standpoint of user roles. The first approach is called *device-centric security management* and the second is called *user-centric security management*. To apply different application settings to different devices, you can use either or both types of management in combination.

Device-centric security management enables you to apply different security application settings to managed devices depending on device-specific features. For example, you can apply different settings to devices allocated in different administration groups.

User-centric security management enables you to apply different security application settings to different user roles. You can create several user roles, assign an appropriate user role to each user, and define different application settings to the devices owned by users with different roles. For example, you may want to apply different application settings to devices of accountants and human resources (HR) specialists. As a result, when user-centric security management is implemented, each department—accounts department and HR department—has its own settings configuration for Kaspersky applications. A settings configuration defines which application settings can be changed by users and which are forcibly set and locked by the administrator.

By using user-centric security management, you can apply specific application settings to individual users. This may be required when an employee has a unique role in the company or when you want to monitor security issues related to devices of a specific person. Depending on the role of this employee in the company, you can expand or limit the rights of this person to change application settings. For example, you might want to expand the rights of a system administrator who manages client devices in a local office.

You can also combine the device-centric and user-centric security management approaches. For example, you can configure a specific application policy for each administration group, and then create policy profiles for one or several user roles of your enterprise. In this case, the policies and policy profiles are applied in the following order:

1. The policies created for device-centric security management are applied.
2. They are modified by the policy profiles according to the policy profile priorities.
3. The policies are modified by the policy profiles associated with user roles.

# Policy setup and propagation: Device-centric approach

When you complete this scenario, the applications will be configured on all of the managed devices in accordance with the application policies and policy profiles that you define.

## Prerequisites

Before you start, make sure that you have installed Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console. You might also want to consider user-centric security management as an alternative or additional option to the device-centric approach. Learn more about two management approaches.

## Stages

The scenario of device-centric management of Kaspersky applications consists of the following steps:

1. **Configuring application policies**

   Configure settings for Kaspersky applications installed on the managed devices by creating a policy for each application. The set of policies will be propagated to the client devices.

   When you configure the protection of your network in quick start wizard, Kaspersky Security Center Linux creates the default policy for the following applications:

   - Kaspersky Endpoint Security for Linux—for Linux-based client devices
   - Kaspersky Endpoint Security for Windows—for Windows-based client devices

   If you completed the configuration process by using this wizard, you do not have to create a new policy for this application.

   If you have a hierarchical structure of several Administration Servers and/or administration groups, the secondary Administration Servers and child administration groups inherit the policies from the primary Administration Server by default. You can force the inheritance by the child groups and secondary Administration Servers to prohibit any modifications of the settings configured in the upstream policy. If you want only part of the settings to be forcibly inherited, you can lock them in the upstream policy. The rest unlocked settings will be available for modification in the downstream policies. The created hierarchy of policies will allow you to effectively manage devices in the administration groups.

   How-to instructions: Creating a policy

2. **Creating policy profiles (optional)**

   If you want devices within a single administration group to run under different policy settings, create policy profiles for those devices. A policy profile is a named subset of policy settings. This subset is distributed on target devices together with the policy, supplementing it under a specific condition called the *profile activation condition*. Profiles only contain settings that differ from the "basic" policy, which is active on the managed device.

   By using profile activation conditions, you can apply different policy profiles, for example, to the devices having a specific hardware configuration or marked with specific tags. Use tags to filter devices that meet specific criteria. For example, you can create a tag called *CentOS*, mark all devices running CentOS operating system with this tag, and then specify this tag as an activation condition for a policy profile. As a result, Kaspersky applications installed on all devices running CentOS will be managed by their own policy profile.

   How-to instructions:

   - Creating a policy profile
   - Creating a policy profile activation rule

3. **Propagating policies and policy profiles to the managed devices**

   By default, the Administration Server automatically synchronizes with managed devices every 15 minutes. During the synchronization, the new or changed policies and policy profiles are propagated to the managed devices. You can circumvent auto-synchronization and run the synchronization manually by using the Force synchronization command. When synchronization is complete, the policies and policy profiles are delivered and applied to the installed Kaspersky applications.

   You can check whether the policies and policy profiles were delivered to a device. Kaspersky Security Center Linux specifies the delivery date and time in the properties of the device.

   How-to instructions: Forced synchronization

### Results

When the device-centric scenario is complete, the Kaspersky applications are configured according to the settings specified and propagated through the hierarchy of policies.

The configured application policies and policy profiles will be applied automatically to the new devices added to the administration groups.

# Policy setup and propagation: User-centric approach

This section describes the scenario of user-centric approach to the centralized configuration of Kaspersky applications installed on the managed devices. When you complete this scenario, the applications will be configured on all of the managed devices in accordance with the application policies and policy profiles that you define.

## Prerequisites

Before you start, make sure that you have successfully installed Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console, and completed the main deployment scenario. You might also want to consider device-centric security management as an alternative or additional option to the user-centric approach. Learn more about two management approaches.

## Process

The scenario of user-centric management of Kaspersky applications consists of the following steps:

1. **Configuring application policies**

   Configure settings for Kaspersky applications installed on the managed devices by creating a policy for each application. The set of policies will be propagated to the client devices.

   When you configure the protection of your network in quick start wizard, Kaspersky Security Center Linux creates the default policy for Kaspersky Endpoint Security. If you completed the configuration process by using this wizard, you do not have to create a new policy for this application.

   If you have a hierarchical structure of several Administration Servers and/or administration groups, the secondary Administration Servers and child administration groups inherit the policies from the primary Administration Server by default. You can force the inheritance by the child groups and secondary Administration Servers to prohibit any modifications of the settings configured in the upstream policy. If you want only part of the settings to be forcibly inherited, you can lock them in the upstream policy. The rest unlocked settings will be available for modification in the downstream policies. The created hierarchy of policies will allow you to effectively manage devices in the administration groups.

   How-to instructions: Creating a policy

2. **Specifying owners of the devices**

   Assign the managed devices to the corresponding users.

   How-to instructions: Assigning a user as a device owner

3. **Defining user roles typical for your enterprise**

   Think about different kinds of work that the employees of your enterprise typically perform. You must divide all employees in accordance with their roles. For example, you can divide them by departments, professions, or positions. After that you will need to create a user role for each group. Keep in mind that each user role will have its own policy profile containing application settings specific for this role.

4. **Creating user roles**

   Create and configure a user role for each group of employees that you defined on the previous step or use the predefined user roles. The user roles will contain set of rights of access to the application features.

   How-to instructions: Creating a user role

5. **Defining the scope of each user role**

   For each of the created user roles, define users and/or security groups and administration groups. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.

   How-to instructions: Editing the scope of a user role

6. **Creating policy profiles**

   Create a policy profile for each user role in your enterprise. The policy profiles define which settings will be applied to the applications installed on users' devices depending on the role of each user.

   How-to instructions: Creating a policy profile

7. **Associating policy profiles with the user roles**

   Associate the created policy profiles with the user roles. After that: the policy profile becomes active for a user that has the specified role. The settings configured in the policy profile will be applied to the Kaspersky applications installed on the user's devices.

   How-to instructions: Associating policy profiles with roles

8. **Propagating policies and policy profiles to the managed devices**

   By default, Kaspersky Security Center Linux automatically synchronizes the Administration Server with the managed devices every 15 minutes. During the synchronization, the new or changed policies and policy profiles are propagated to the managed devices. You can circumvent auto-synchronization and run the synchronization manually by using the Force synchronization command. When synchronization is complete, the policies and policy profiles are delivered and applied to the installed Kaspersky applications.

   You can check whether the policies and policy profiles were delivered to a device. Kaspersky Security Center Linux specifies the delivery date and time in the properties of the device.

   How-to instructions: Forced synchronization

Results

When the user-centric scenario is complete, the Kaspersky applications are configured according to the settings specified and propagated through the hierarchy of policies and policy profiles.

For a new user, you will have to create a new account, assign the user one of the created user roles, and assign the devices to the user. The configured application policies and policy profiles will be automatically applied to the devices of this user.

# Policies and policy profiles

In Kaspersky Security Center Web Console, you can create policies for Kaspersky applications. This section describes policies and policy profiles, and provides instructions for creating and modifying them.

## About policies and policy profiles

A *policy* is a set of Kaspersky application settings that are applied to an administration group and its subgroups. You can install several Kaspersky applications on the devices of an administration group. Kaspersky Security Center provides a single policy for each Kaspersky application in an administration group. A policy has one of the following statuses:

The status of the policy

| State | Description |
|---|---|
| Active | The current policy that is applied to the device. Only one policy may be active for a Kaspersky application in each administration group. Devices apply the settings values of an active policy for a Kaspersky application. |
| Inactive | A policy that is not currently applied to a device. |
| Out-of-office | If this option is selected, the policy becomes active when the device leaves the corporate network. |

Policies function according to the following rules:

- Multiple policies with different values can be configured for a single application.
- Only one policy can be active for the current application.
- A policy can have child policies.

Generally, you can use policies as preparations for emergency situations, such as a virus attack. For example, if there is an attack via flash drives, you can activate a policy that blocks access to flash drives. In this case, the current active policy automatically becomes inactive.

In order to prevent maintaining multiple policies, for example, when different occasions assume changing of several settings only, you may use policy profiles.

A *policy profile* is a named subset of policy settings values that replaces the settings values of a policy. A policy profile affects the effective settings formation on a managed device. *Effective settings* are a set of policy settings, policy profile settings, and local application settings that are currently applied for the device.

Policy profiles function according to the following rules:

- A policy profile takes effect when a specific activation condition occurs.
- Policy profiles contain values of settings that differ from the policy settings.
- Activation of a policy profile changes the effective settings of the managed device.
- A policy can include a maximum of 100 policy profiles.

# About lock and locked settings

Each policy setting has a lock button icon (). The table below shows lock button statuses:

Lock button statuses

| State | Description |
|---|---|
| Undefined | If an open lock is displayed next to a setting and the toggle button is disabled, the setting is not specified in the policy. A user can change these settings in the managed application interface. These type of settings are called *unlocked*. |
| Enforce | If a closed lock is displayed next to a setting and the toggle button is enabled, the setting is applied to the devices where the policy is enforced. A user cannot modify the values of these settings in the managed application interface. These type of settings are called *locked*. |

We highly recommend that you close locks for the policy settings that you want to apply on the managed devices. The unlocked policy settings can be reassigned by Kaspersky application settings on a managed device.

You can use a lock button for performing the following actions:

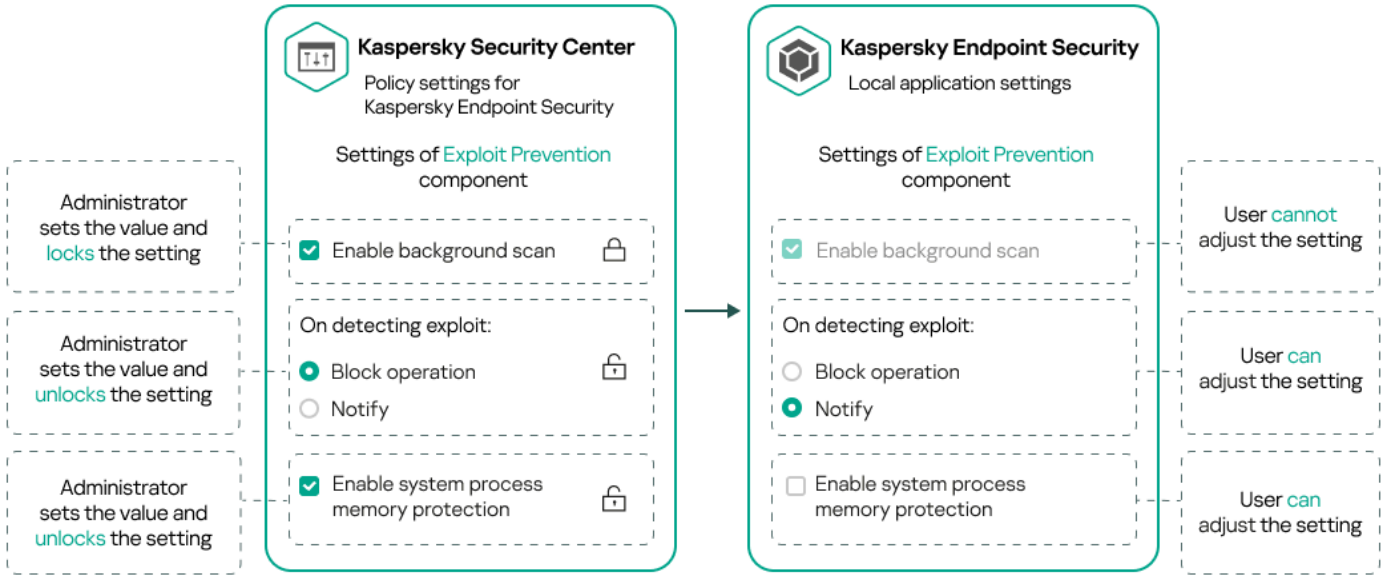
- Locking settings for an administration subgroup policy
- Locking settings of a Kaspersky application on a managed device

Thus, a locked setting is used for implementing effective settings on a managed device.

A process of effective settings implementation includes the following actions:

- Managed device applies settings values of Kaspersky application.
- Managed device applies locked settings values of a policy.

A policy and managed Kaspersky application contain the same set of settings. When you configure policy settings, the Kaspersky application settings change values on a managed device. You cannot adjust locked settings on a managed device (see the figure below):




Locks and Kaspersky application settings

# Inheritance of policies and policy profiles

This section provides information about the hierarchy and inheritance of policies and policy profiles.

## Hierarchy of policies

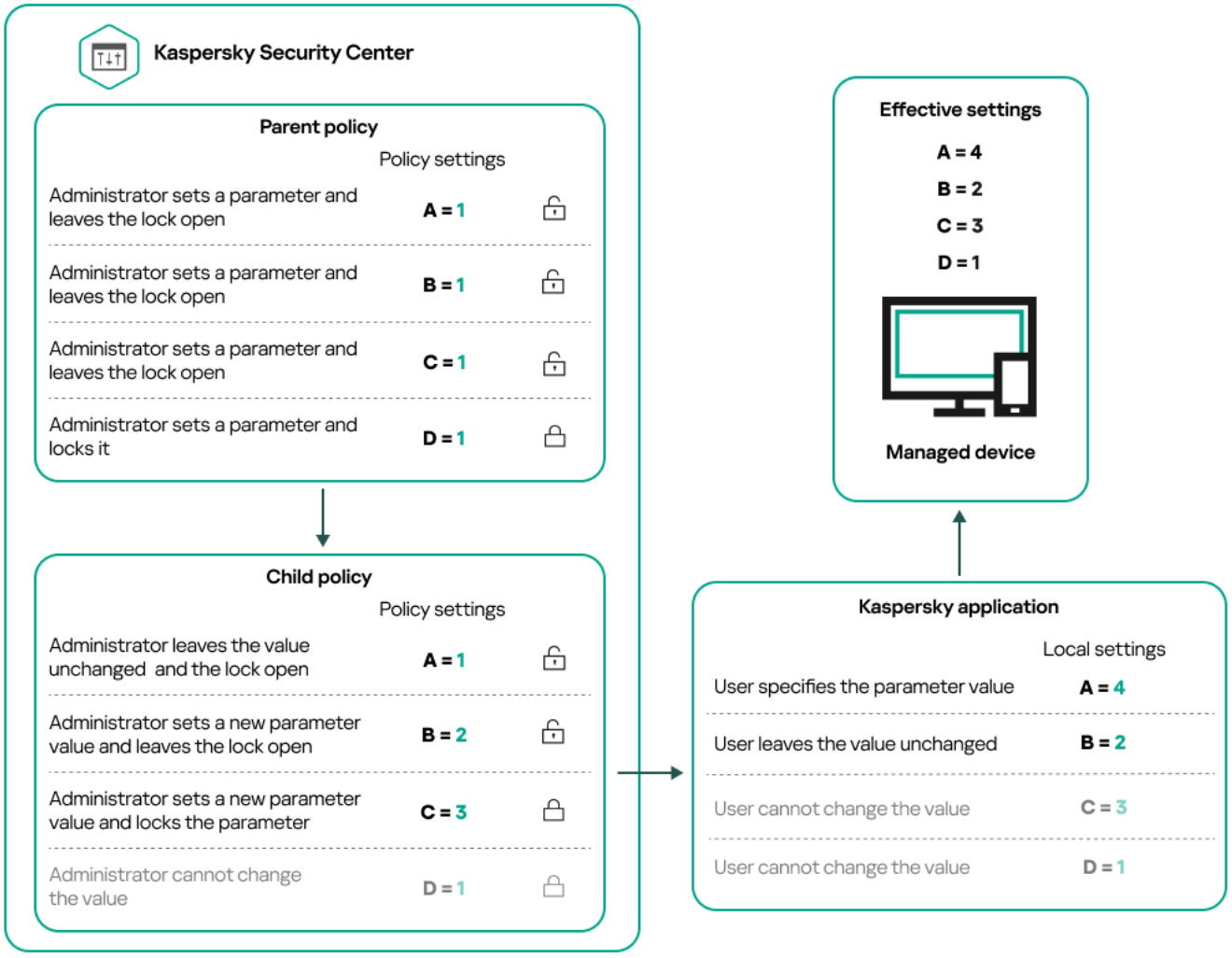
If different devices need different settings, you can organize devices into administration groups.

You can specify a policy for a single administration group. Policy settings can be *inherited*. Inheritance means receiving policy settings values in subgroups (child groups) from a policy of a higher-level (parent) administration group.

Hereinafter, a policy for a parent group is also referred to as a *parent policy*. A policy for a subgroup (child group) is also referred to as a *child policy*.

By default, at least one managed devices group exists on Administration Server. If you want to create custom groups, they are created as subgroups (child groups) within the managed devices group.

Policies of the same application act on each other, according to a hierarchy of administration groups. Locked settings from a policy of a higher-level (parent) administration group will reassign policy settings values of a subgroup (see the figure below).

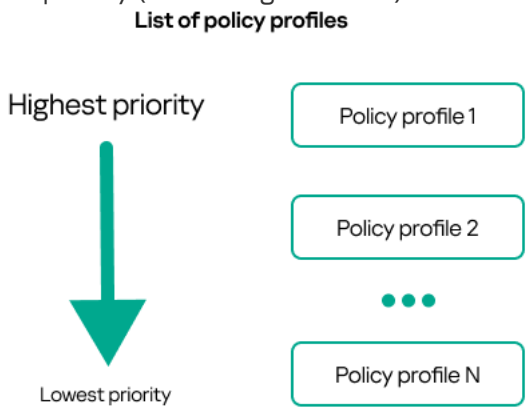



Hierarchy of policies

# Policy profiles in a hierarchy of policies

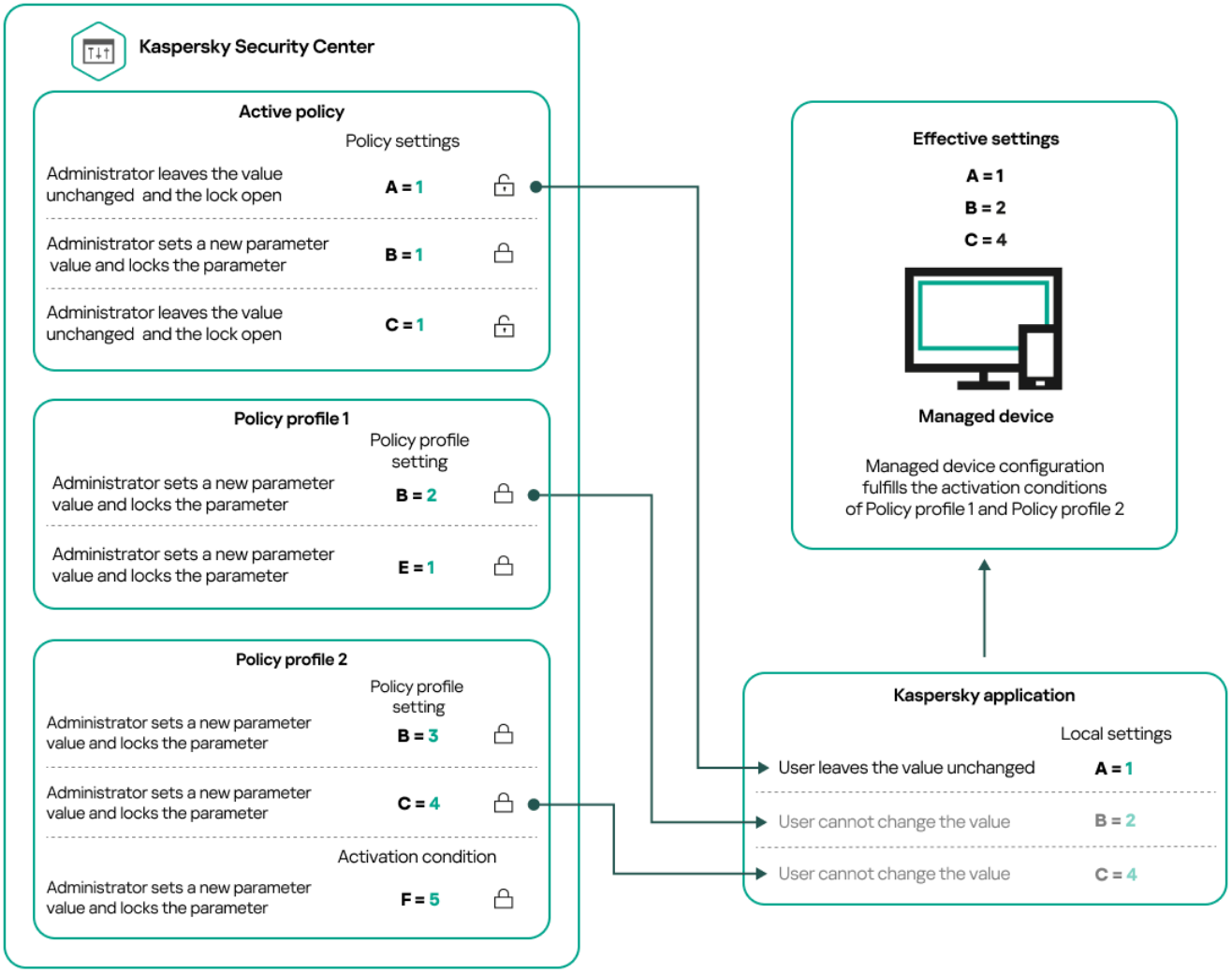
Policy profiles have the following priority assignment conditions:

- A profile's position in a policy profile list indicates its priority. You can change a policy profile priority. The highest position in a list indicates the highest priority (see the figure below).




Priority definition of a policy profile

- Activation conditions of policy profiles do not depend on each other. Several policy profiles can be activated simultaneously. If several policy profiles affect the same setting, the device takes the setting value from the policy profile with the highest priority (see the figure below).

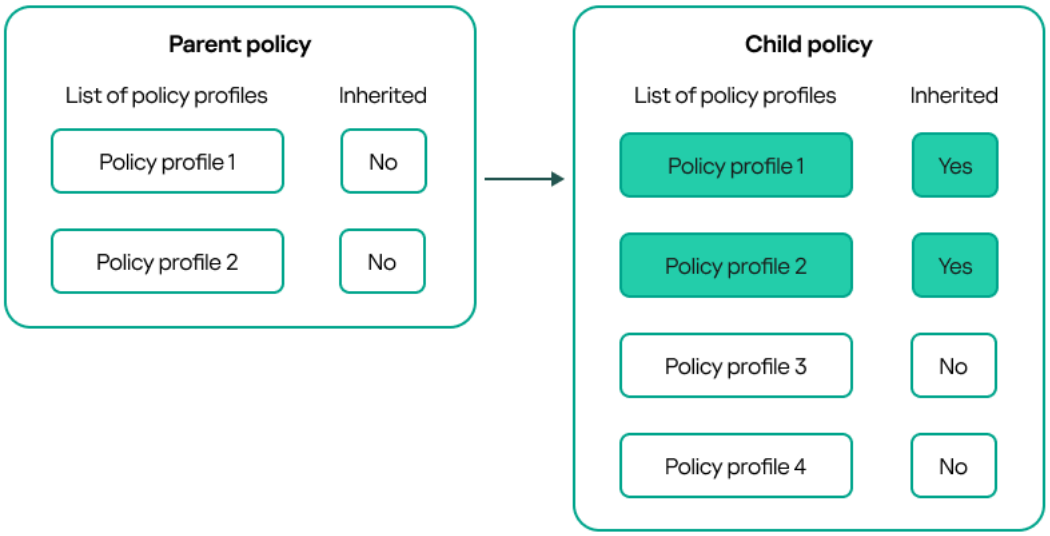



Managed device configuration fulfills activation conditions of several policy profiles

Policy profiles in a hierarchy of inheritance

Policy profiles from different hierarchy level policies comply with the following conditions:

- A lower-level policy inherits policy profiles from a higher-level policy. A policy profile inherited from a higher-level policy obtains higher priority than the original policy profile's level.
- You cannot change a priority of an inherited policy profile (see the figure below).

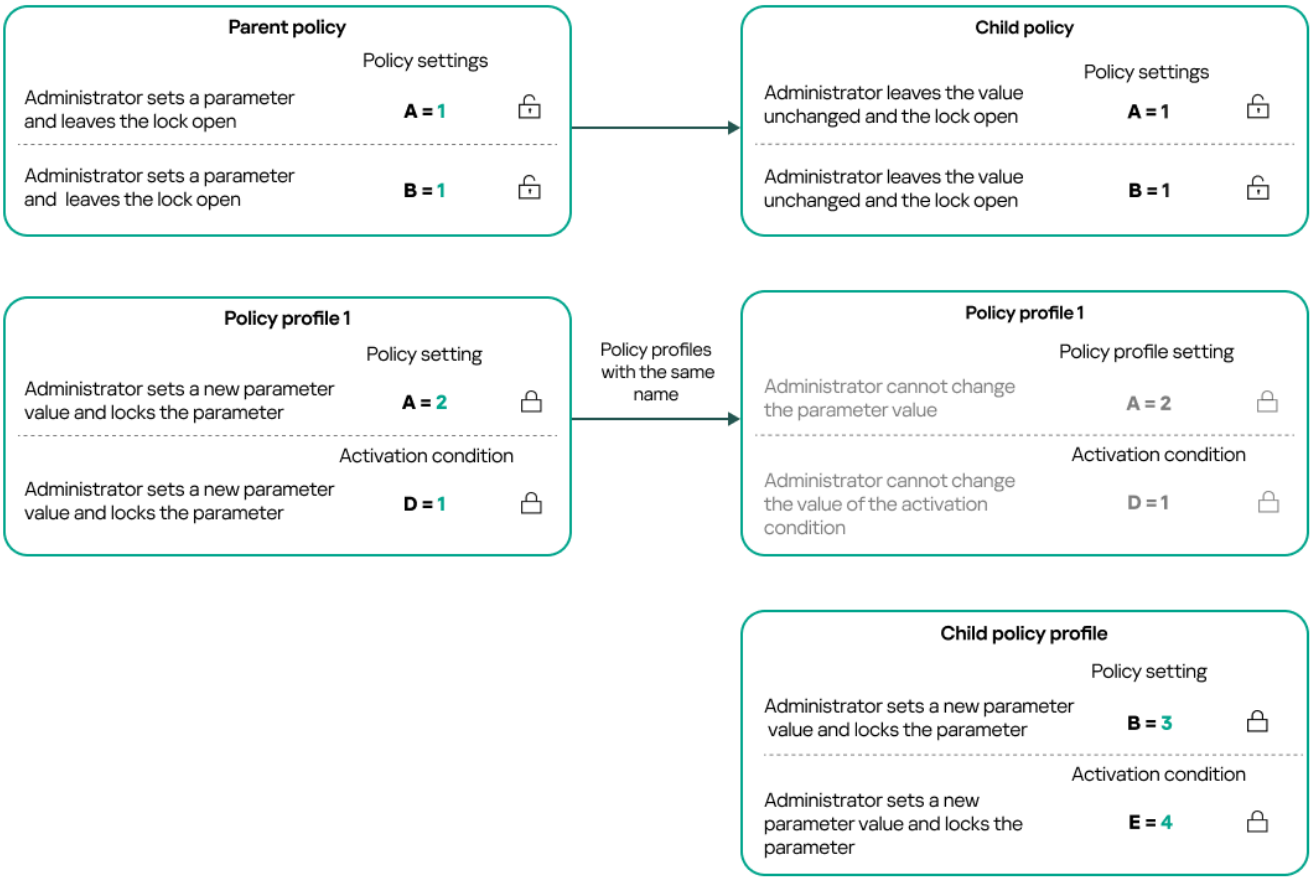



Inheritance of policy profiles

Policy profiles with the same name

If there are two policies with the same names in different hierarchy levels, these policies function according to the following rules:

- Locked settings and the profile activation condition of a higher-level policy profile changes the settings and profile activation condition of a lower-level policy profile (see the figure below).




Child profile inherits settings values from a parent policy profile

- Unlocked settings and the profile activation condition of a higher-level policy profile do not change the settings and profile activation condition of a lower-level policy profile.

## How settings are implemented on a managed device

Implementation of effective settings on a managed device can be described as follows:

- The values of all settings that have not been locked are taken from the policy.
- Then they are overwritten with the values of managed application settings.
- And then the locked settings values from the effective policy are applied. Locked settings values change the values of unlocked effective settings.

# Managing policies

This section describes managing policies and provides information about viewing the list of policies, creating a policy, modifying a policy, copying a policy, moving a policy, forced synchronization, viewing the policy distribution status chart, and deleting a policy.

## Viewing the list of policies

You can view lists of policies created for the Administration Server or for any administration group.

*To view a list of policies:*

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. In the administration group structure, select the administration group for which you want to view the list of policies.

The list of policies appears in tabular format. If there are no policies, the table is empty. You can show or hide the columns of the table, change their order, view only lines that contain a value that you specify, or use search.

## Creating a new policy

You can create policies; you can also modify and delete existing policies.

*To create a policy:*

1. In the main menu, go to **Asset management** → **Policies**.
2. Select the administration group for which the policy is to be created:
   - For the root group.

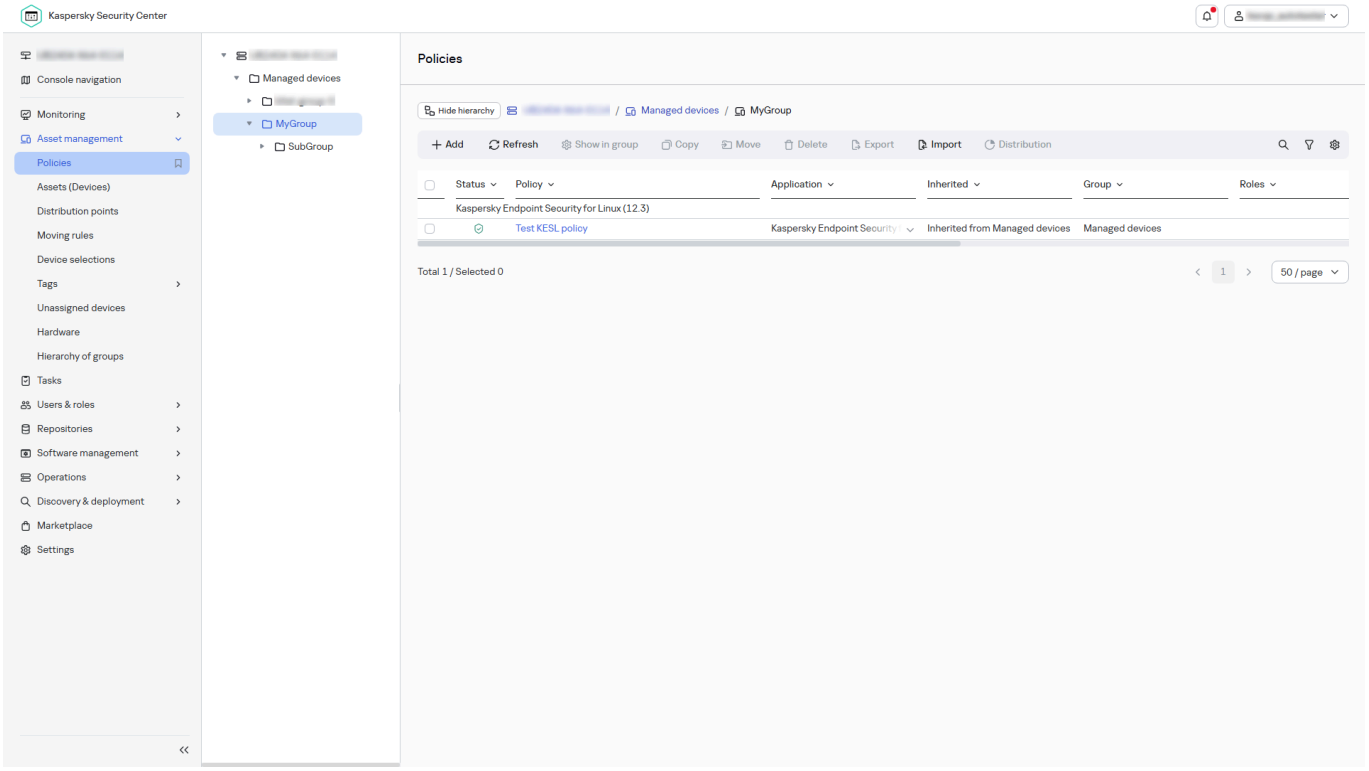
     In this case you can proceed to the next step.
   - For a subgroup:

     a. Click the **Show hierarchy** button at the top of the page.

     The button name changes to **Hide hierarchy**.

     b. In the window that opens, click the name of the required subgroup.

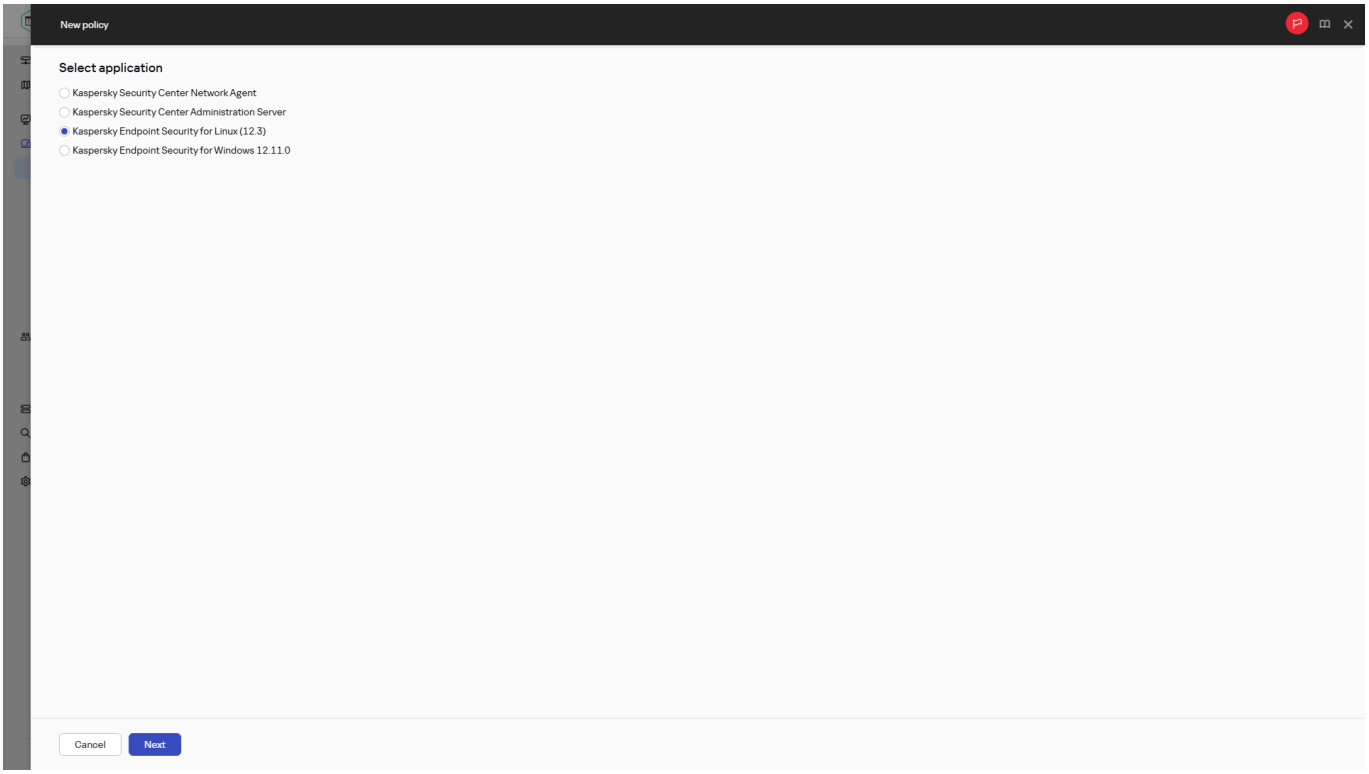
The path to the selected group is displayed at the top of the page. If necessary, you can click a link with the administration group name to go to the group. By default, the last link in the path is inactive. Also, you can close the hierarchy window by clicking the **Hide hierarchy** button.




The list of policies

3. Click **Add**.

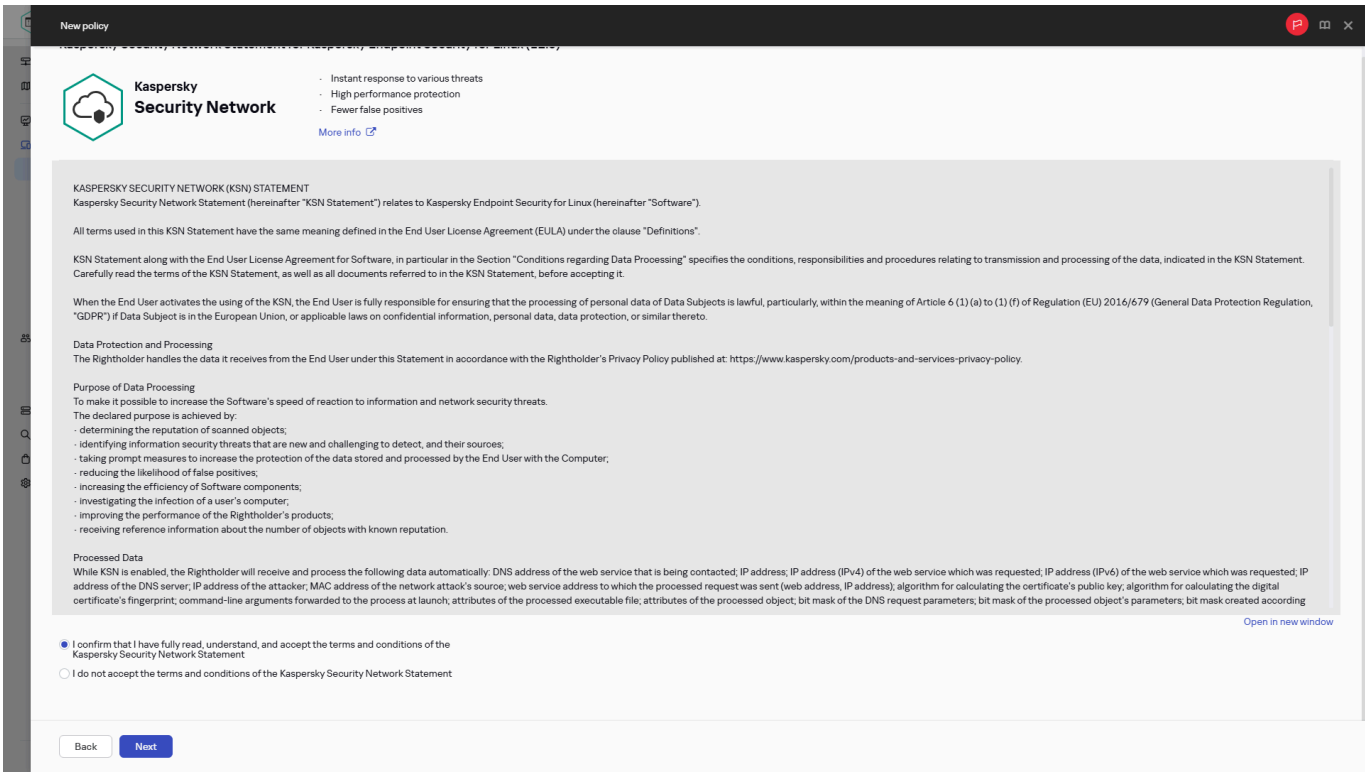
   The **Select application** window opens.




Creating a new policy

4. Select the application for which you want to create a policy.

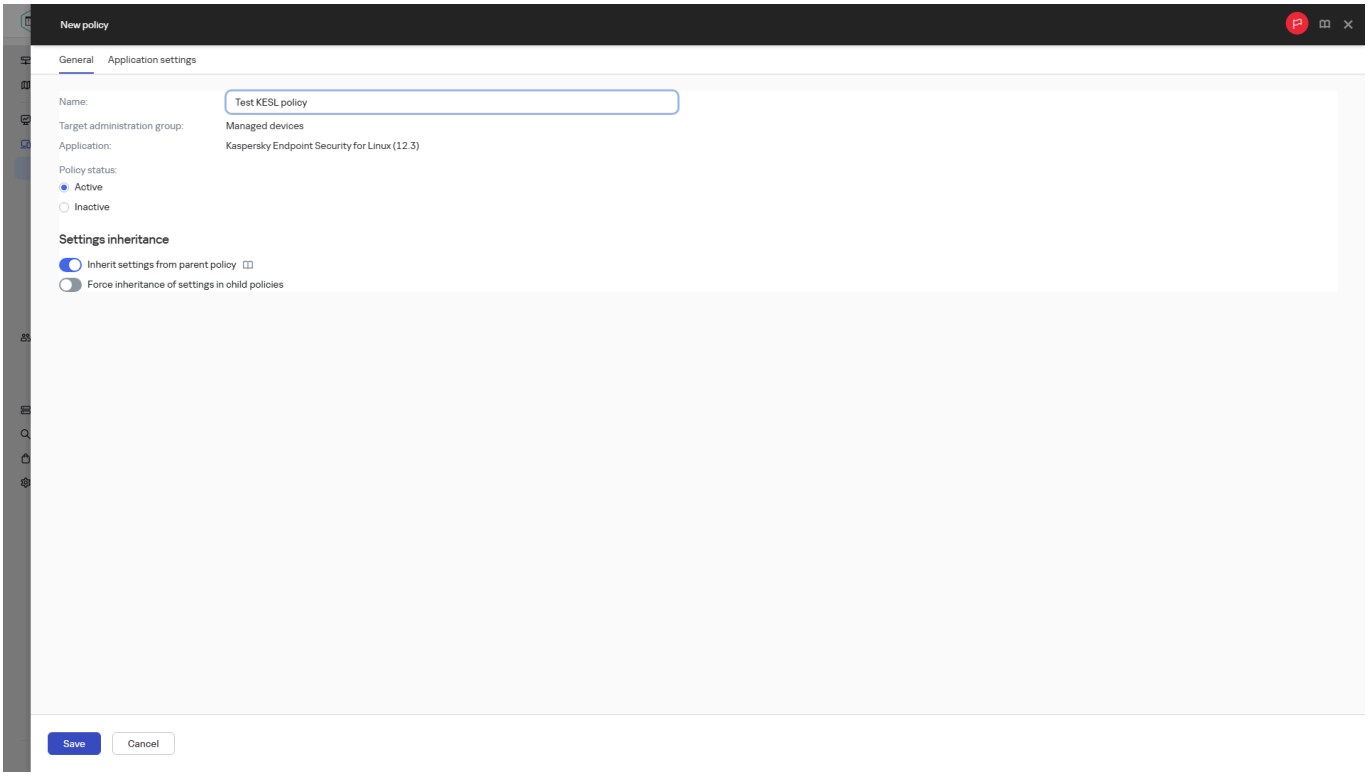
5. If Kaspersky Security Network is supported by the Kaspersky application, for which you are creating a policy, you will be prompted to accept the KSN Statement. If you want to use Kaspersky Security Network, accept the KSN Statement.




Accepting the KSN Statement

6. Click **Next**.

The new policy settings window opens with the **General** tab selected. If you want, change the default name, default status, and default inheritance settings of the policy.




The new policy settings window

7. Select the **Application settings** tab.

Or, you can click **Save** and exit. The policy will appear in the list of policies, and you can edit its settings later.

8. On the **Application settings** tab, in the left pane select the category that you want and in the results' pane on the right, edit the settings of the policy. You can edit policy settings in each category (section).

   The set of settings depends on the application for which you create a policy. For details, refer to the following:

   - Configuring Administration Server
   - Network Agent policy settings
   - Kaspersky Endpoint Security for Linux Help
   - Kaspersky Endpoint Security for Windows Help

   For details about settings of other security applications, refer to the documentation for the corresponding application.

   When editing the settings, you can click **Cancel** to cancel the last operation.

9. Click **Save** to save the policy.

   A notification is displayed with the following message: **The policy is being saved and distributed through the hierarchy of Administration Servers**.

   If the policy passes validation, the following notification is displayed: **Policy has been saved**.

   If the policy fails validation, the following notification is displayed: **Failed to save and distribute the policy through the Administration Servers hierarchy. Contact Technical Support**. You can review and revise the policy settings, and then try again. If the issue persists, contact Technical Support.

The policy will appear in the list of policies. Once the policy is created, policy change events are exported to SIEM system, if this option is enabled.

# General policy settings

General

In the **General** tab, you can modify the policy status and specify the inheritance of policy settings:

- In the **Policy status** block, you can select one of the policy modes:

  **Active**

  If this option is selected, the policy becomes active.

  By default, this option is selected.

  **Out-of-office**

  If this option is selected, the policy becomes active when the device leaves the corporate network.

  **Inactive**

  If this option is selected, the policy becomes inactive, but it is still stored in the **Policies** folder. If required, the policy can be activated.

- In the **Settings inheritance** settings group, you can configure the policy inheritance:

  **Inherit settings from parent policy**

If this option is enabled, the policy setting values are inherited from the upper-level group policy and, therefore, are locked.

By default, the option is enabled.

**Force inheritance of settings in child policies**

If this option is enabled, after policy changes are applied, the following actions will be performed:

- The values of the policy settings will be propagated to the policies of administration subgroups, that is, to the child policies.
- In the **Settings inheritance** block of the **General** section in the properties window of each child policy, the **Inherit settings from parent policy** option will be automatically enabled.

If this option is enabled, the child policies settings are locked.

By default, this option is disabled.

## Event configuration

The **Event configuration** tab allows you to configure event logging and event notification. Events are distributed by importance level on the following tabs:

- **Critical**

  The **Critical** section is not displayed in the Network Agent policy properties.

- **Functional failure**
- **Warning**
- **Info**

In each section, the list shows the types of events and the default event storage period on the Administration Server (in days). Clicking an event type lets you specify the following settings:

- **Event registration**

  You can specify how many days to store the event and select where to store the event:

  - **Export to SIEM system by using Syslog**
  - **Store in the OS event log on device**
  - **Store in the OS event log on Administration Server**

- **Event notifications**

  You can select if you want to be notified about the event in one of the following ways:

  - **Notify by email**
  - **Notify by SMS**
  - **Notify by running an executable file or script**
  - **Notify by SNMP**

By default, the notification settings specified on the Administration Server properties tab (such as recipient address) are used. If you want, you can change these settings in the **Email**, **SMS**, and **Executable file to be run** tabs.

Also, the **Event configuration** tab displays a notification when new event types are added (for example, in a new version of the application), and enables you to apply the new settings by clicking the **Save** or **Save and close** button.

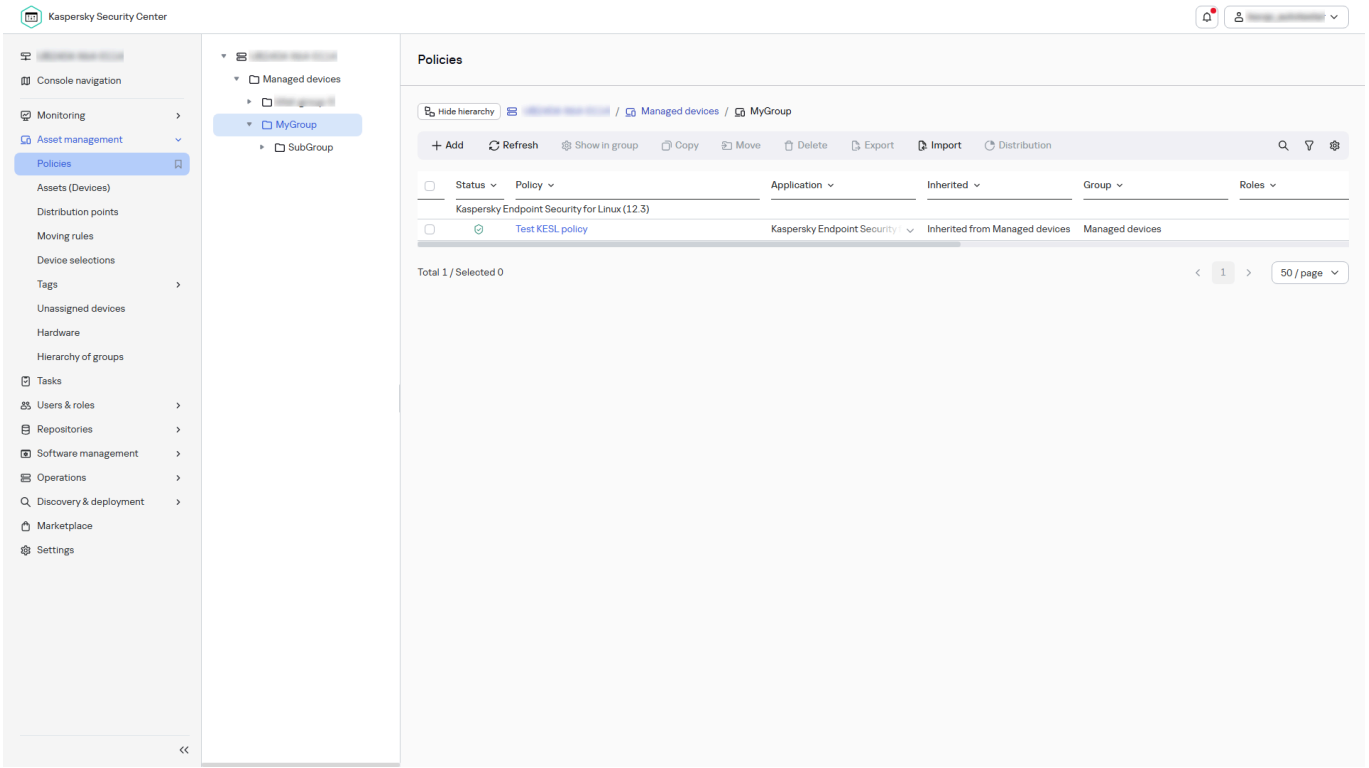
Revision history

The **Revision history** tab allows you to view the list of the policy revisions, compare the policy revisions, and roll back changes made to the policy, if necessary.

# Modifying a policy

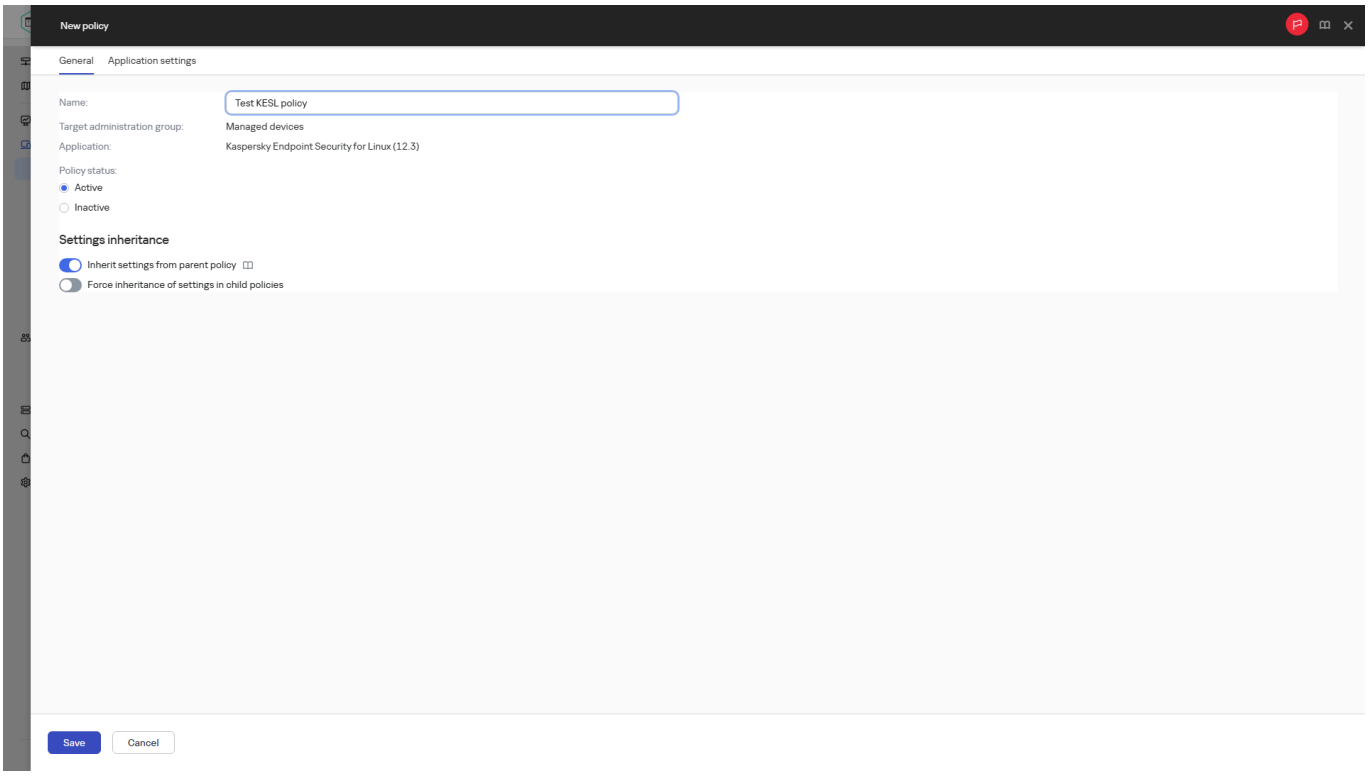
*To modify a policy:*

1. In the main menu, go to **Asset management** → **Policies**.




2. Click the policy that you want to modify.

   The policy settings window opens.




3. Specify the general settings and settings of the application for which you create a policy. For details, refer to the following:

   - Configuring Administration Server
   - Network Agent policy settings
   - Kaspersky Endpoint Security for Linux Help
   - Kaspersky Endpoint Security for Windows Help

   For details about settings of other security applications, refer to the documentation for that application.

4. Click the **Save** button.

   A notification is displayed with the following message: **The policy is being saved and distributed through the hierarchy of Administration Servers**.

   If the policy passes validation, the following notification is displayed: **Policy has been saved**.

   If the policy fails validation, the following notification is displayed: **Failed to save and distribute the policy through the Administration Servers hierarchy. Contact Technical Support**. You can review and revise the policy settings, and then try again. If the issue persists, contact Technical Support.

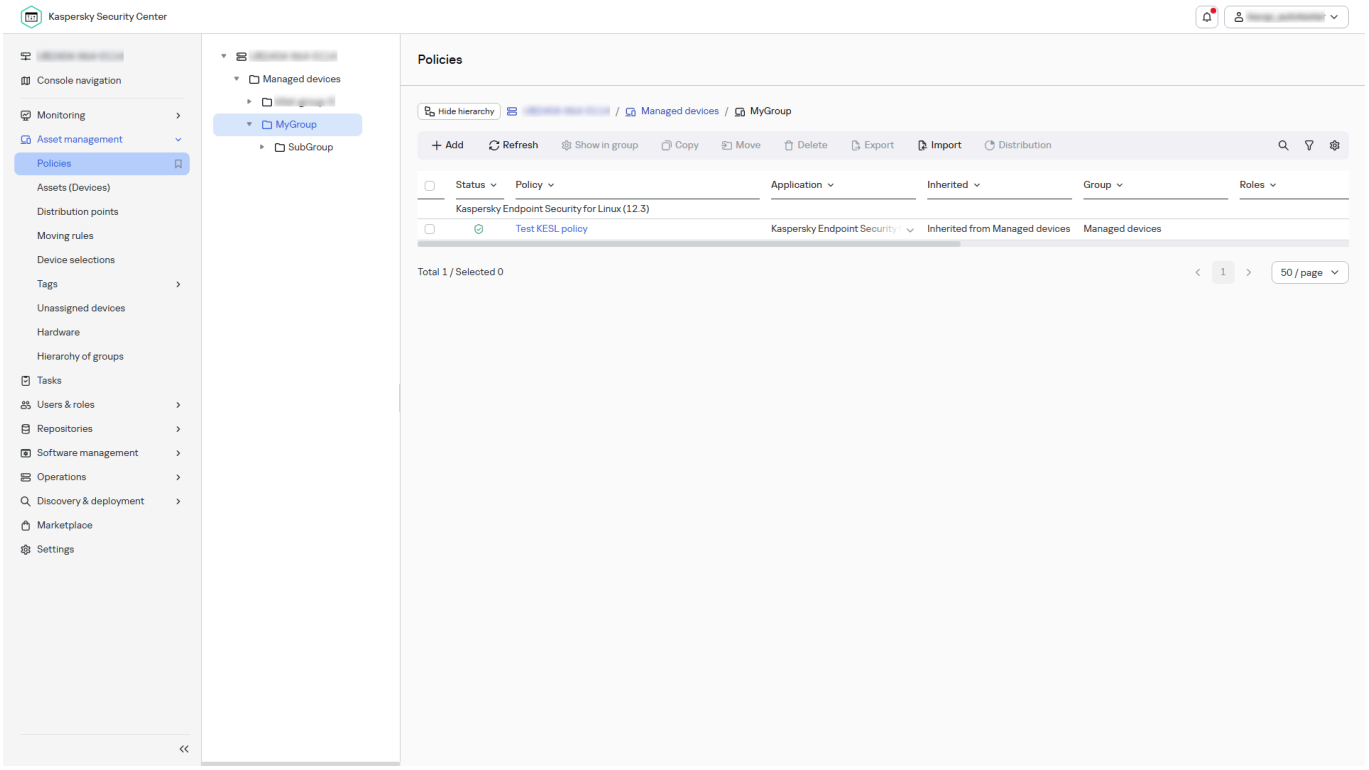
The changes made to the policy will be saved in the policy properties, and will appear in the **Revision history** section. Once the policy is modified, policy change events are exported to SIEM system, if this option is enabled.

If necessary, you can compare policy revisions. The option is available for the policies of Administration Server, Network Agent, Kaspersky Endpoint Security for Windows (starting from 14.0 web plug-in version), and Kaspersky Endpoint Security for Mac (starting from 12.2.1 Patch A web plug-in version).

# Enabling and disabling a policy inheritance option

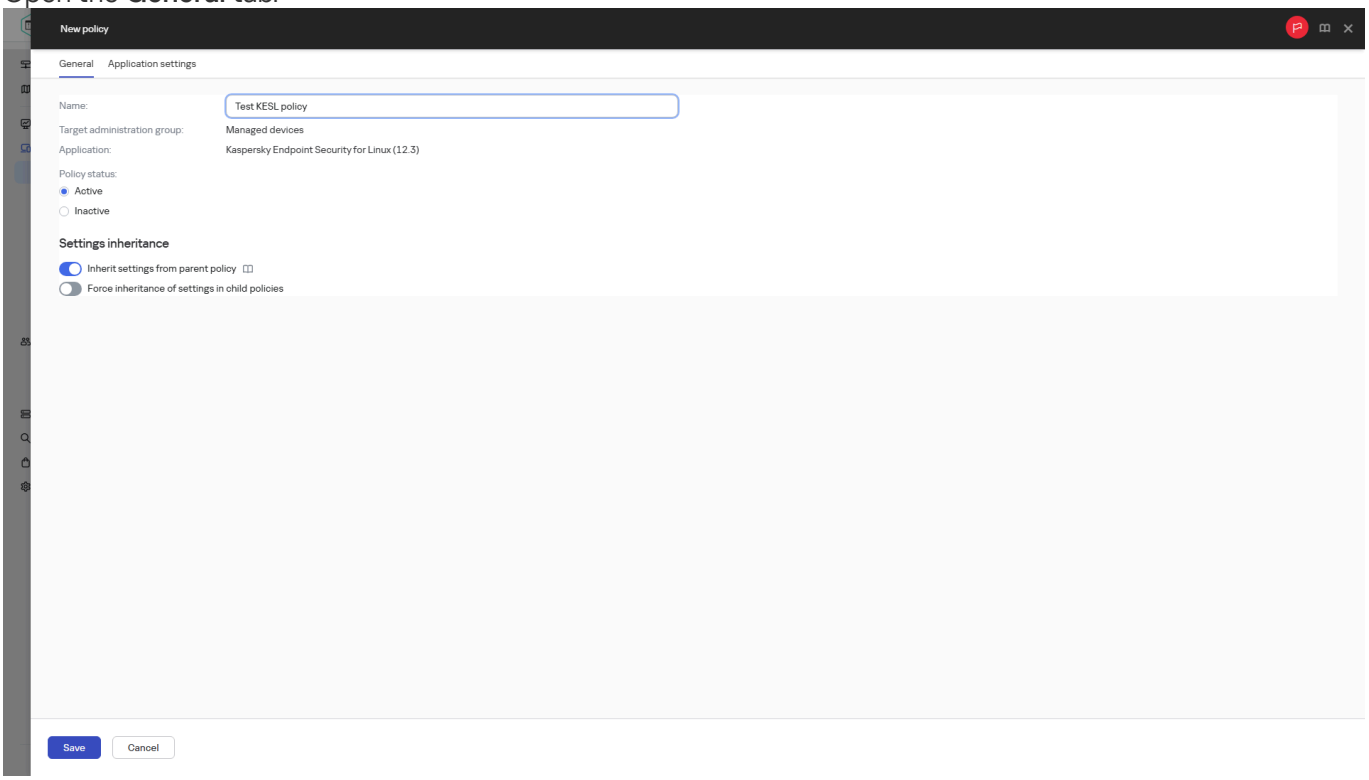
*To enable or disable the inheritance option in a policy:*

1. Open the required policy.




The list of policies

2. Open the **General** tab.



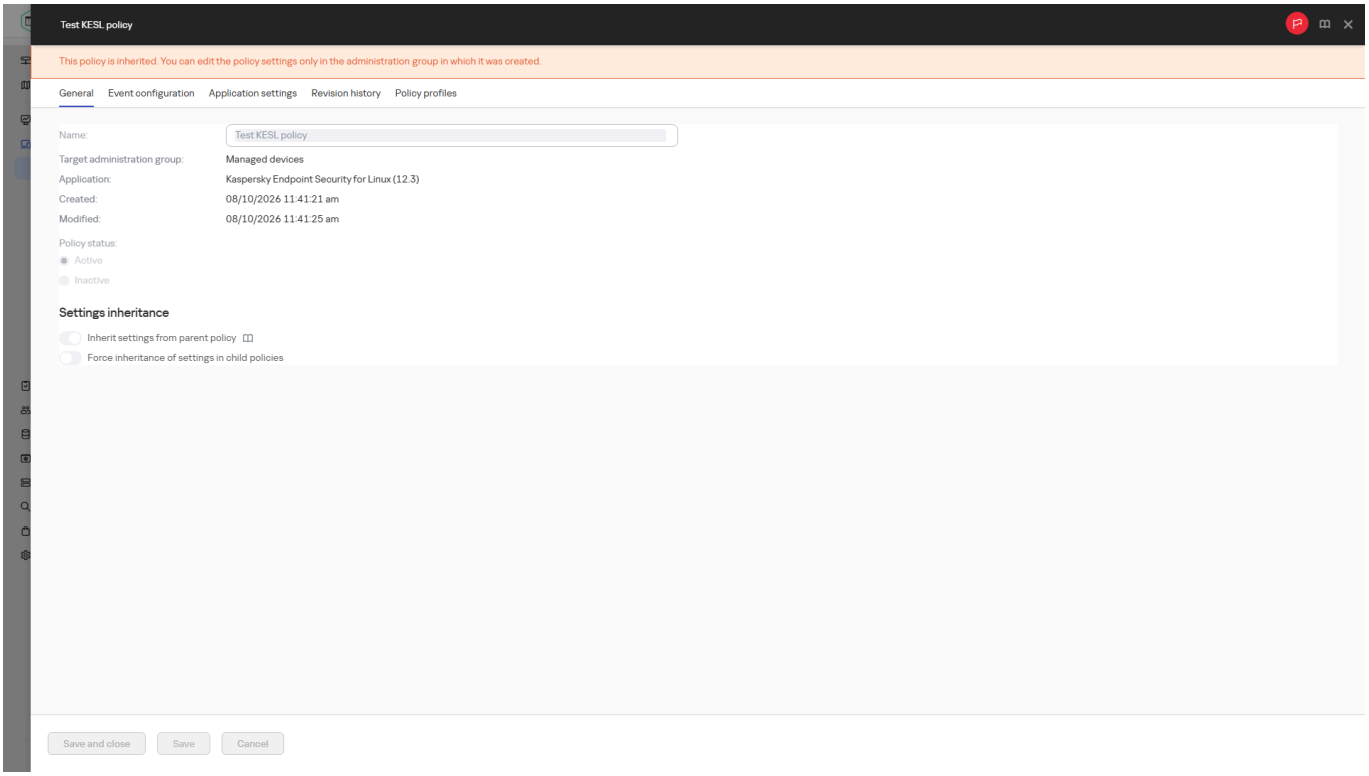

Creating a new policy

3. Enable or disable policy inheritance:

   - If you enable **Inherit settings from parent policy** in a child policy and an administrator locks some settings in the parent policy, then you cannot change these settings in the child policy.

   - If you disable **Inherit settings from parent policy** in a child policy, then you can change all of the settings in the child policy, even if some settings are locked in the parent policy.

   - If you enable **Force inheritance of settings in child policies** in the parent group, this enables the **Inherit settings from parent policy** option for each child policy. In this case, you cannot disable this option for any child policy. All of the settings that are locked in the parent policy are forcibly inherited in the child groups, and you cannot change these settings in the child groups.




Locked policy settings

4. Click the **Save** button to save changes or click the **Cancel** button to reject changes.

By default, the **Inherit settings from parent policy** option is enabled for a new policy.

If a policy has profiles, all of the child policies inherit these profiles.

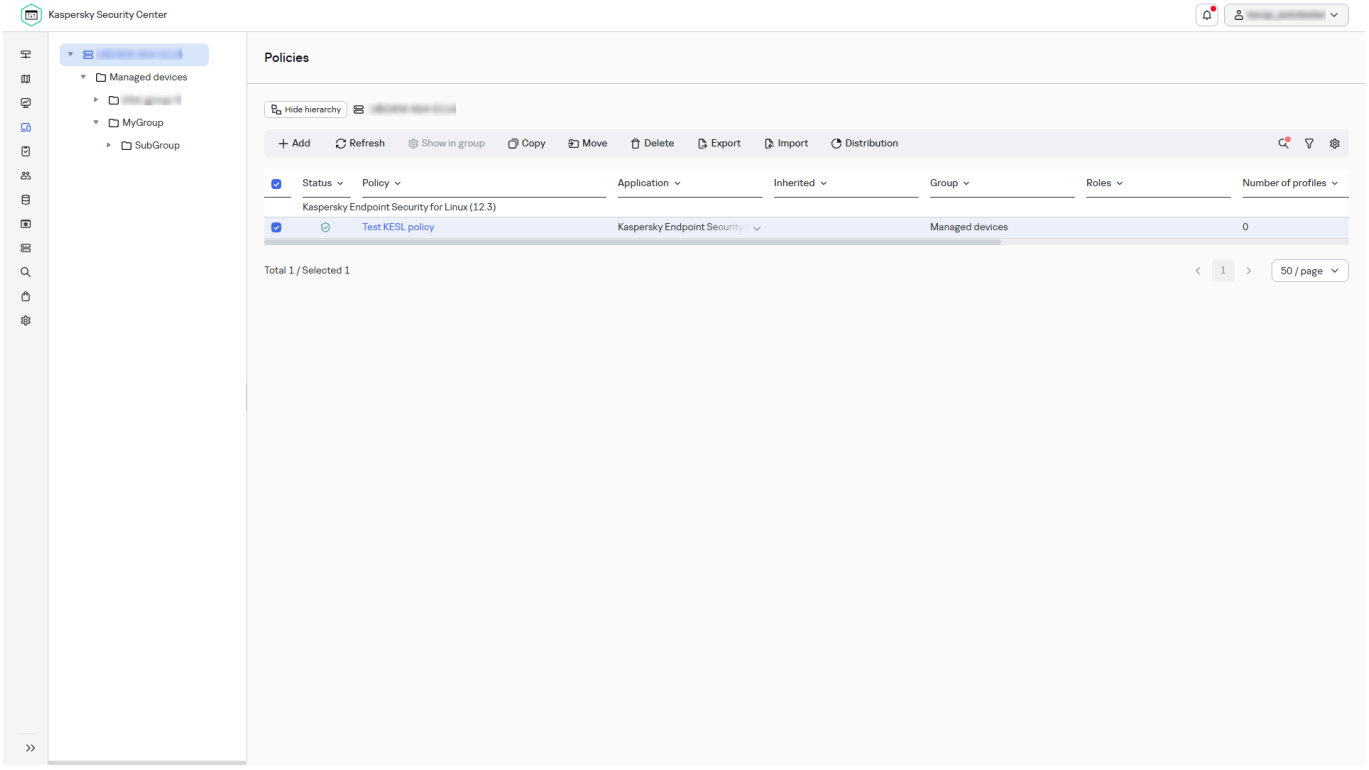
## Copying a policy

You can copy policies from one administration group to another.

*To copy a policy to another administration group:*

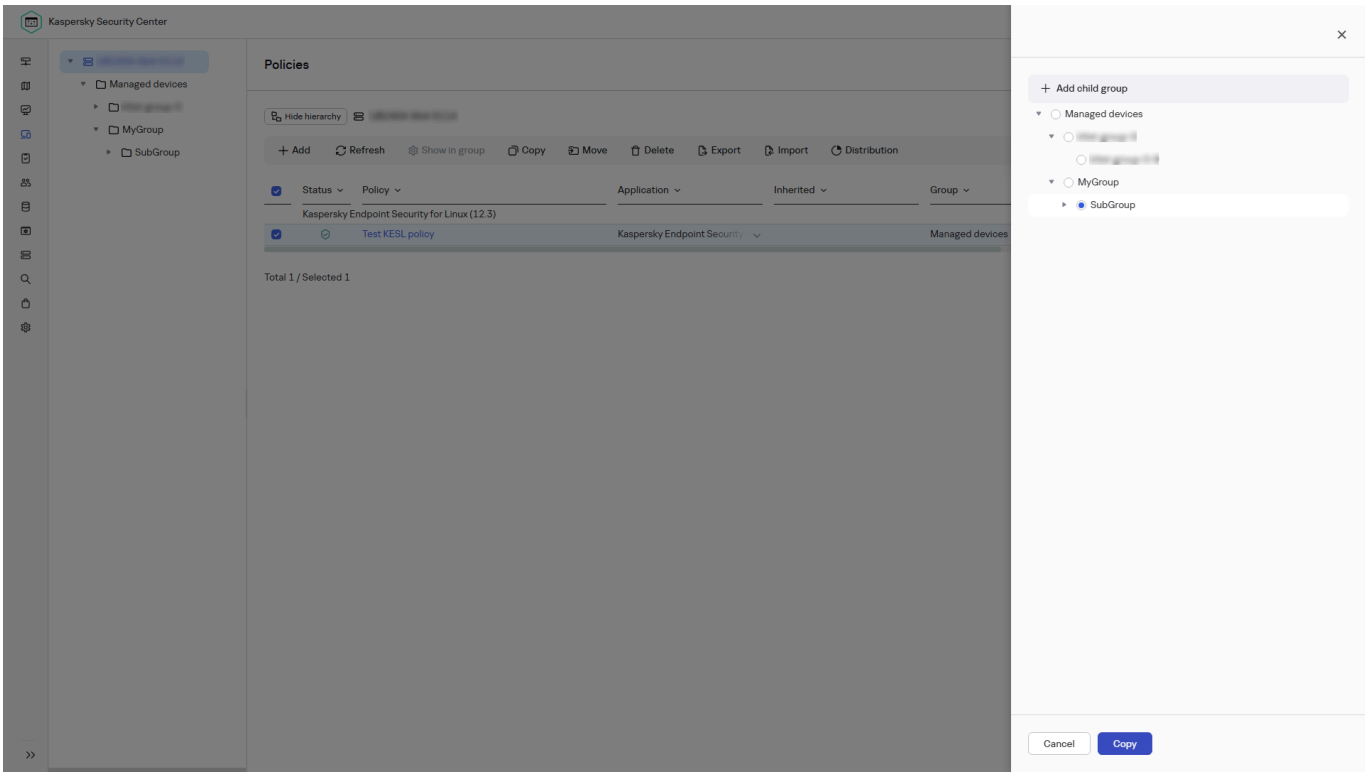
1. In the main menu, go to **Asset management** → **Policies**.

2. Select the check box next to the policy (or policies) that you want to copy.




3. Click **Copy**.

   On the right side of the screen, the tree of the administration groups appears.




4. In the tree, select the target group, that is, the group to which you want to copy the policy (or policies).

5. Click the **Copy** button at the bottom of the screen.

6. Click **OK** to confirm the operation.

The policy (policies) will be copied to the target group with all its profiles. The status of each copied policy in the target group will be **Inactive**. You can change the status to **Active** at any time.

If a policy with the name identical to that of the newly moved policy already exists in the target group, the name of the newly moved policy is expanded with the (<next sequence number>) index, for example: (1).

## Moving a policy

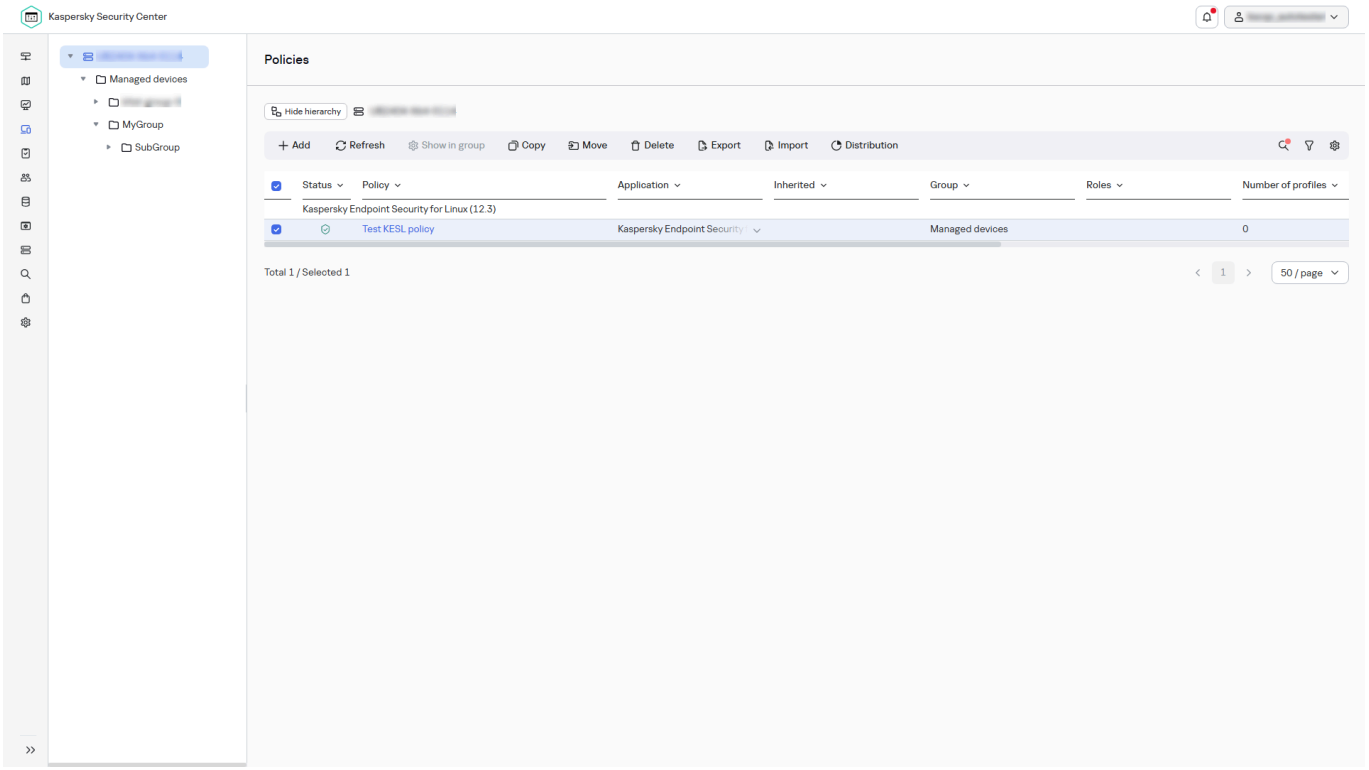
You can move policies from one administration group to another. For example, you want to delete a group, but you want to use its policies for another group. In this case, you may want move the policy from the old group to the new one before deleting the old group.

> When moving a policy to another administration group, the revision history of the policy is cleared. The **Revision history** tab displays information about the latest change only.

*To move a policy to another administration group:*

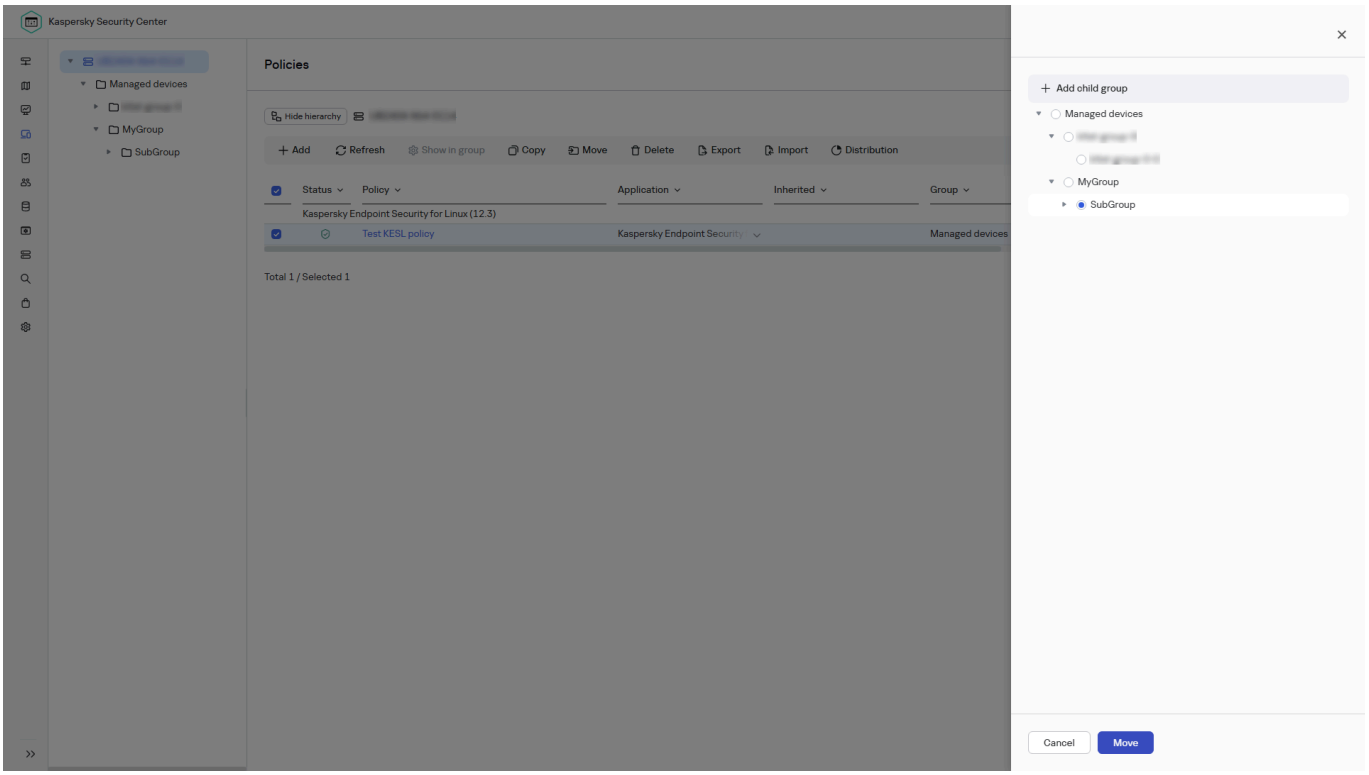
1. In the main menu, go to **Asset management** → **Policies**.

2. Select the check box next to the policy (or policies) that you want to move.




3. Click the **Move** button.

   On the right side of the screen, the tree of the administration groups appears.




4. In the tree, select the target group, that is, the group to which you want to move the policy (or policies).

5. Click the **Move** button at the bottom of the screen.

6. Click **OK** to confirm the operation.

   If a policy is not inherited from the source group, it is moved to the target group with all its profiles. The status of the policy in the target group is **Inactive**. You can change the status to **Active** at any time.

   If a policy is inherited from the source group, it remains in the source group. It is copied to the target group with all its profiles. The status of the policy in the target group is **Inactive**. You can change the status to **Active** at any time.

If a policy with the name identical to that of the newly moved policy already exists in the target group, the name of the newly moved policy is expanded with the (<next sequence number>) index, for example: (1).

## Exporting a policy

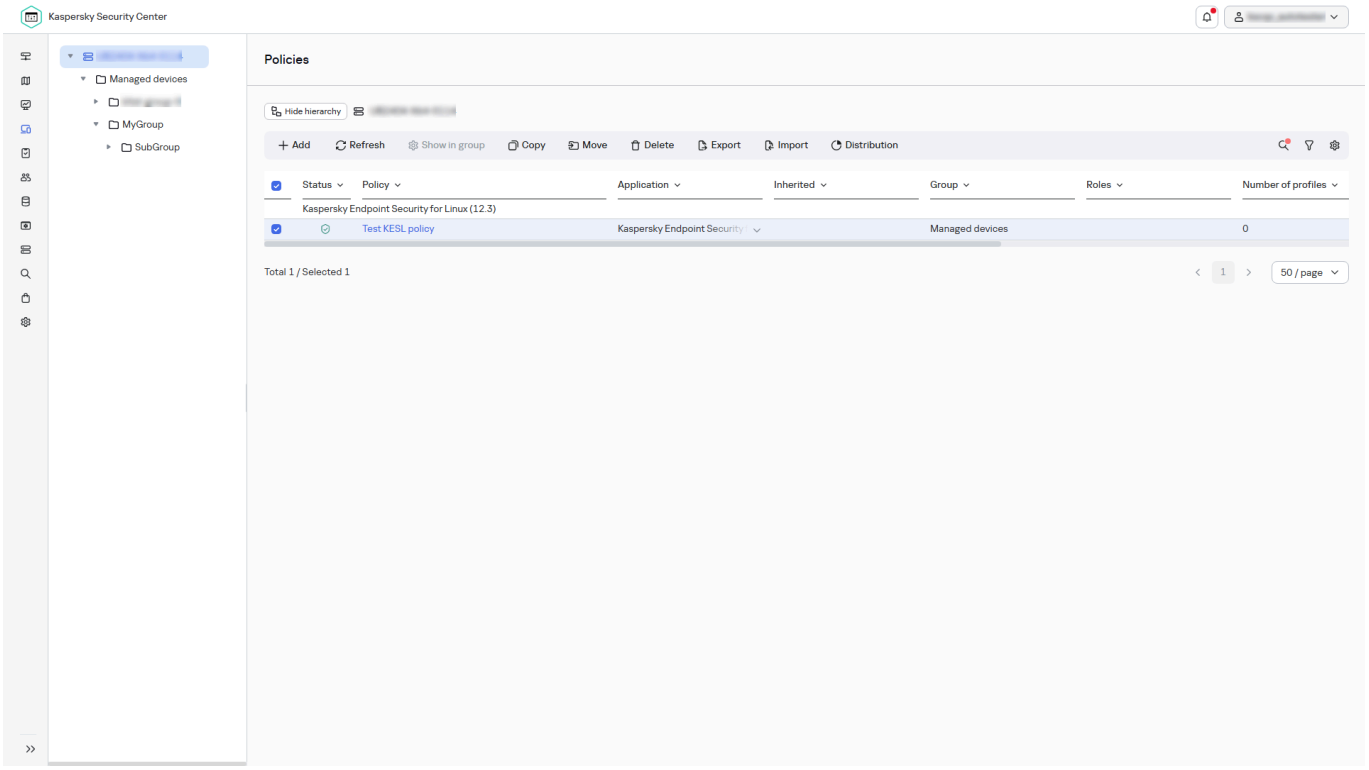
Kaspersky Security Center Linux allows you to save a policy, its settings, and the policy profiles to a KLP file. You can use this KLP file to import the saved policy both to Kaspersky Security Center Windows and Kaspersky Security Center Linux.

*To export a policy:*

1. In the main menu, go to **Asset management** → **Policies**.

2. Select the check box next to the policy that you want to export.

You cannot export multiple policies at the same time. If you select more than one policy, the **Export** button will be disabled.




Selecting a policy for export

3. Click the **Export** button.

4. In the opened **Save as** window, specify the policy file name and path. Click the **Save** button.

   The **Save as** window is displayed only if you use Google Chrome, Microsoft Edge, or Opera. If you use another browser, the policy file is automatically saved in the **Downloads** folder.

## Importing a policy

Kaspersky Security Center Linux allows you to import a policy from a KLP file. The KLP file contains the exported policy, its settings, and the policy profiles.

*To import a policy:*

1. In the main menu, go to **Asset management** → **Policies**.

2. Click the **Import** button.

3. Click the **Browse** button to choose a policy file that you want to import.

4. In the opened window, specify the path to the KLP policy file, and then click the **Open** button. Note that you can select only one policy file.

   The policy processing starts.

5. After the policy is processed successfully, select the administration group to which you want to apply the policy.

6. Click the **Complete** button to finish the policy import.

The notification with the import results appears. If the policy is imported successfully, you can click the **Details** link to view the policy properties.

After a successful import, the policy is displayed in the policy list. The settings and profiles of the policy are also imported. Regardless of the policy status that was selected during the export, the imported policy is inactive. You can change the policy status in the policy properties.

If the application policy settings contain passwords, such a policy cannot be applied after being imported to another Administration Server. In this case, change the passwords in the imported policy to apply it.

If the newly imported policy has a name identical to that of an existing policy, the name of the imported policy is expanded with the **(<next sequence number>)** index, for example: **(1)**, **(2)**.

## Forced synchronization

Although Kaspersky Security Center Linux automatically synchronizes the status, settings, tasks, and policies for managed devices, in some cases the administrator must know for certain, at a given moment, whether synchronization has already been performed for a specified device.

### Synchronizing a single device

*To force synchronization between the Administration Server and a managed device:*

1. In the main menu, go to **Asset management** → **Managed devices**.
2. Click the name of the device that you want to synchronize with the Administration Server.

   A property window opens with the **General** section selected.
3. Click the **Force synchronization** button.

The application synchronizes the selected device with the Administration Server.

### Synchronizing multiple devices

*To force synchronization between the Administration Server and multiple managed devices:*

1. Open the device list of an administration group or a device selection:
   - Run a device selection to view the device list.
   - In the main menu, go to **Asset management** → **Managed devices**, and then select the administration group that contains devices to synchronize:
     - For the root group, you can proceed to the next step.
     - For a subgroup, click the **Show hierarchy** button at the top of the page, and then in the window that opens, click the name of the subgroup.

       The path to the selected group is displayed at the top of the page. If necessary, you can click a link with the administration group name to go to the group. By default, the last link in the path is inactive. Also, you can close the hierarchy window by clicking the **Hide hierarchy** button.
2. Select the check boxes next to the devices that you want to synchronize with the Administration Server.
3. Above the list of managed devices, click the ellipsis button ( ... ), then click the **Force synchronization** button.

   The application synchronizes the selected devices with the Administration Server.
4. In the device list, check that the time of last connection to the Administration Server has changed, for the selected devices, to the current time. If the time has not changed, update the page content by clicking the **Refresh** button.

The selected devices are synchronized with the Administration Server.

### Viewing the time of a policy delivery

After changing a policy for a Kaspersky application on the Administration Server, the administrator can check whether the changed policy has been delivered to a specific managed device. A policy can be delivered during a regular synchronization or a forced synchronization.

*To view the date and time that an application policy was delivered to a managed device:*

1. In the main menu, go to **Asset management** → **Managed devices**.
2. Click the name of the device that you want to synchronize with the Administration Server.

   A property window opens with the **General** section selected.
3. Click the **Applications** tab.
4. Select the application for which you want to view the policy synchronization date.

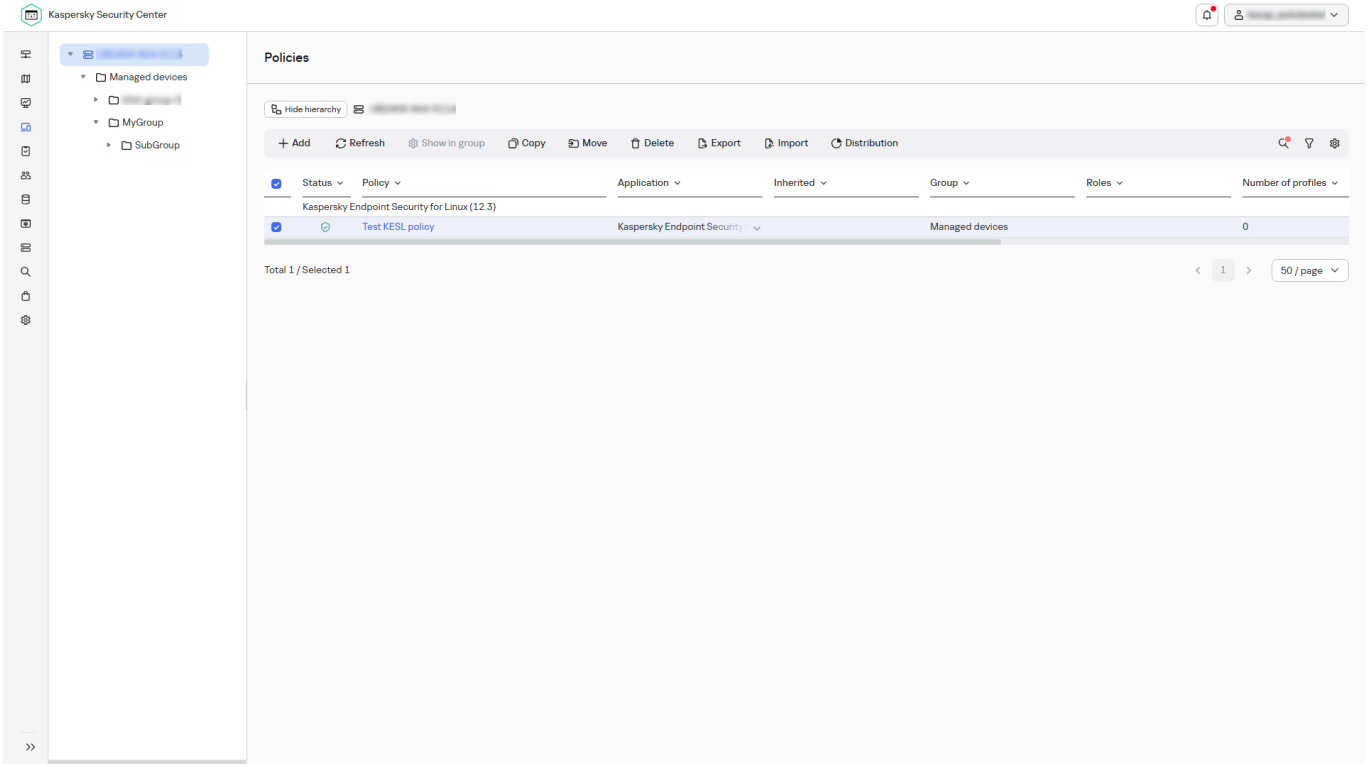
   The application policy window opens with the **General** section selected and the policy delivery date and time displayed.

# Viewing the policy distribution status chart

In Kaspersky Security Center Linux, you can view the status of policy application on each device in a policy distribution status chart.

*To view the policy distribution status on each device:*

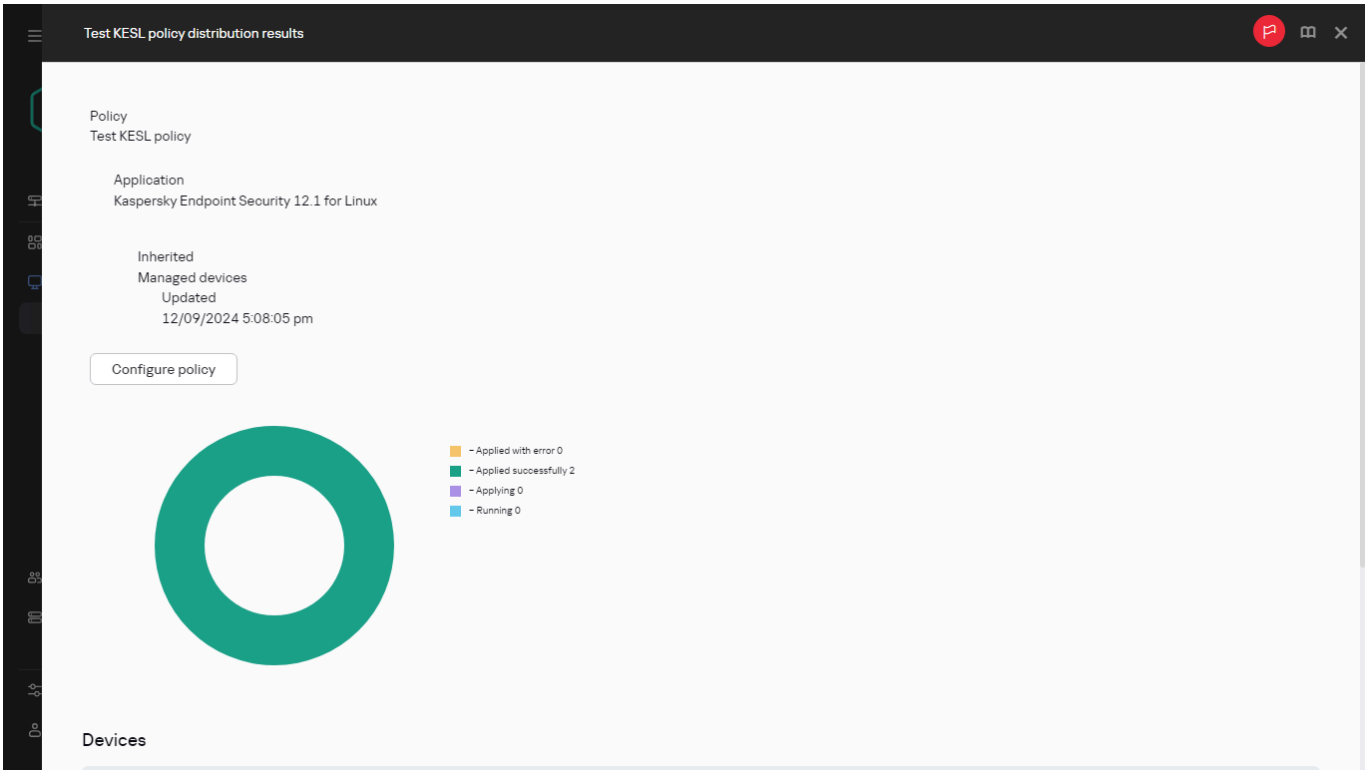
1. In the main menu, go to **Asset management** → **Policies**.
2. Select check box next to the name of the policy for which you want to view the distribution status on devices.




The list of policies

3. In the menu that appears, select the **Distribution** link.

The **<Policy name> distribution results** window opens.




The distribution results of the policy

4. In the **<Policy name> distribution results** window that opens, the **Status description** of the policy is displayed.

You can change number of results displayed in the list with policy distribution. The maximum number of devices is 100,000.

*To change the number of devices displayed in the list with policy distribution results:*

1. In the main menu, go to **Settings** → **Interface options**.
2. In the **Limit of devices displayed in policy distribution results**, enter the number of devices (up to 100,000).

   By default, the number is 5000.
3. Click the **Save** button.

   The settings are saved and applied.

## Activating a policy automatically at the Virus outbreak event

*To make a policy perform automatic activation at a Virus outbreak event:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens, with the **General** tab selected.
2. Select the **Virus outbreak** section.
3. In the right pane, click the **Configure policies to activate when a virus outbreak event occurs** link.

   The **Policy activation** window opens.

4. In the section relating to the component that detects a virus outbreak—Anti-Virus for workstations and file servers, Anti-Virus for mail servers, or Anti-Virus for perimeter defense—select the option button next to the entry you want, and then click **Add**.

   A window opens with the **Managed devices** administration group.

5. Click the chevron icon (>) next to **Managed devices**.

   A hierarchy of administration groups and their policies is displayed.

6. In the hierarchy of administration groups and their policies, click the name of a policy or policies that are activated when a virus outbreak is detected.

   To select all policies in the list or in a group, select the check box next to the required name.

7. Click the **Save** button.

   The window with the hierarchy of administration groups and their policies is closed.

The selected policies are added to the list of policies that are activated when a virus outbreak is detected. The selected policies are activated at the virus outbreak, independent whether they are active or inactive.

If a policy has been activated on the Virus outbreak event, you can return to the previous policy only by using the manual mode.

## Deleting a policy

You can delete a policy if you do not need it anymore. You can delete only a policy that is not inherited in the specified administration group. If a policy is inherited, you can only delete it in the upper-level group for which it was created.

*To delete a policy:*

1. In the main menu, go to **Asset management** → **Policies**.

2. Select the check box next to the policy that you want to delete, and click **Delete**.

   The **Delete** button becomes unavailable (dimmed) if you select an inherited policy.

3. Click **OK** to confirm the operation.

The policy is deleted together with all its profiles. Once the policy is deleted, policy change events are exported to SIEM system, if this option is enabled.

# Managing policy profiles

This section describes managing policy profiles and provides information about viewing the profiles of a policy, changing a policy profile priority, creating a policy profile, copying a policy profile, creating a policy profile activation rule, deleting, exporting and importing a policy profile.

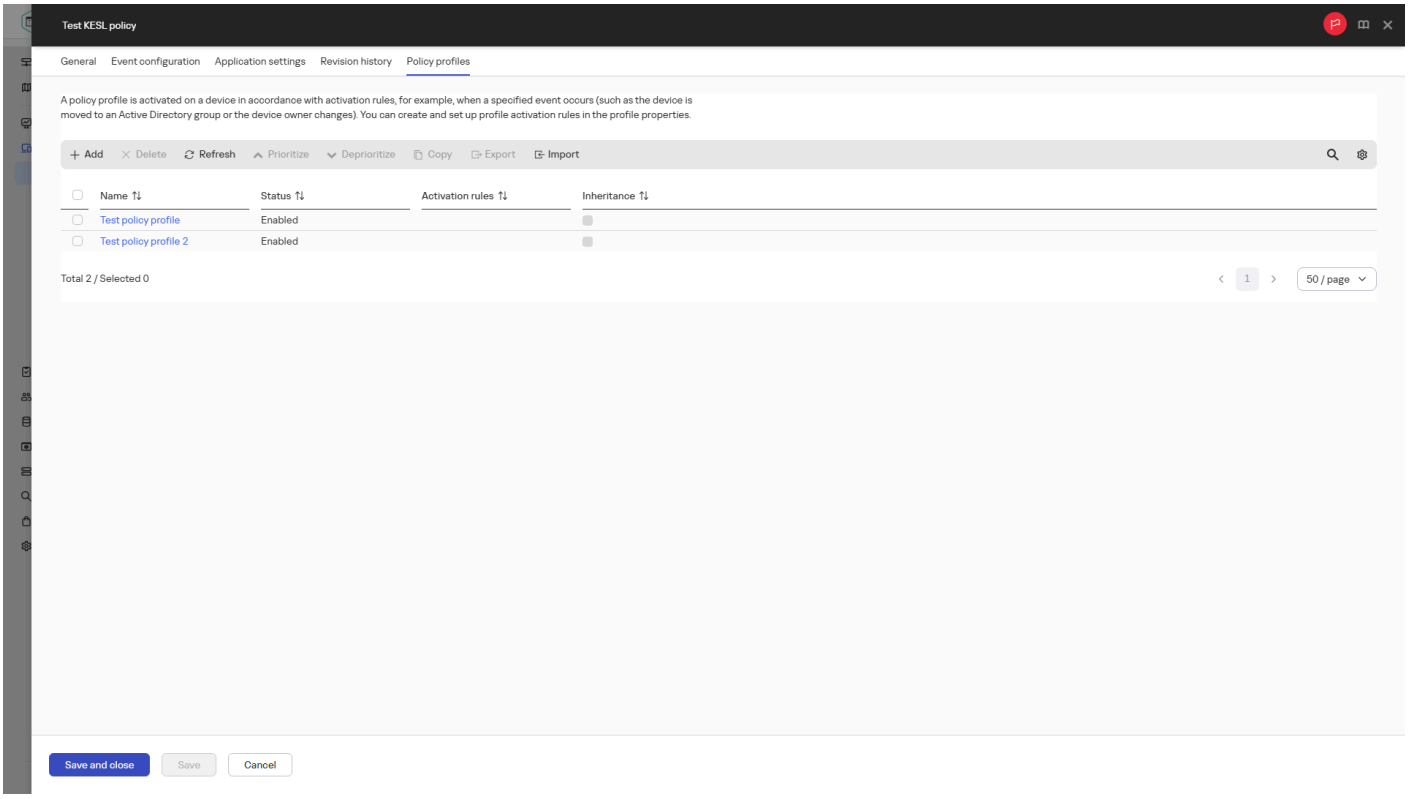
# Viewing the profiles of a policy

*To view profiles of a policy:*

1. In the main menu, go to **Asset management** → **Policies**.
2. Click the name of the policy whose profiles you want to view.

   The policy properties window opens with the **General** tab selected.
3. Open the **Policy profiles** tab.

The list of policy profiles appears in tabular format. If the policy does not have profiles, an empty table appears.




The list of policy profiles

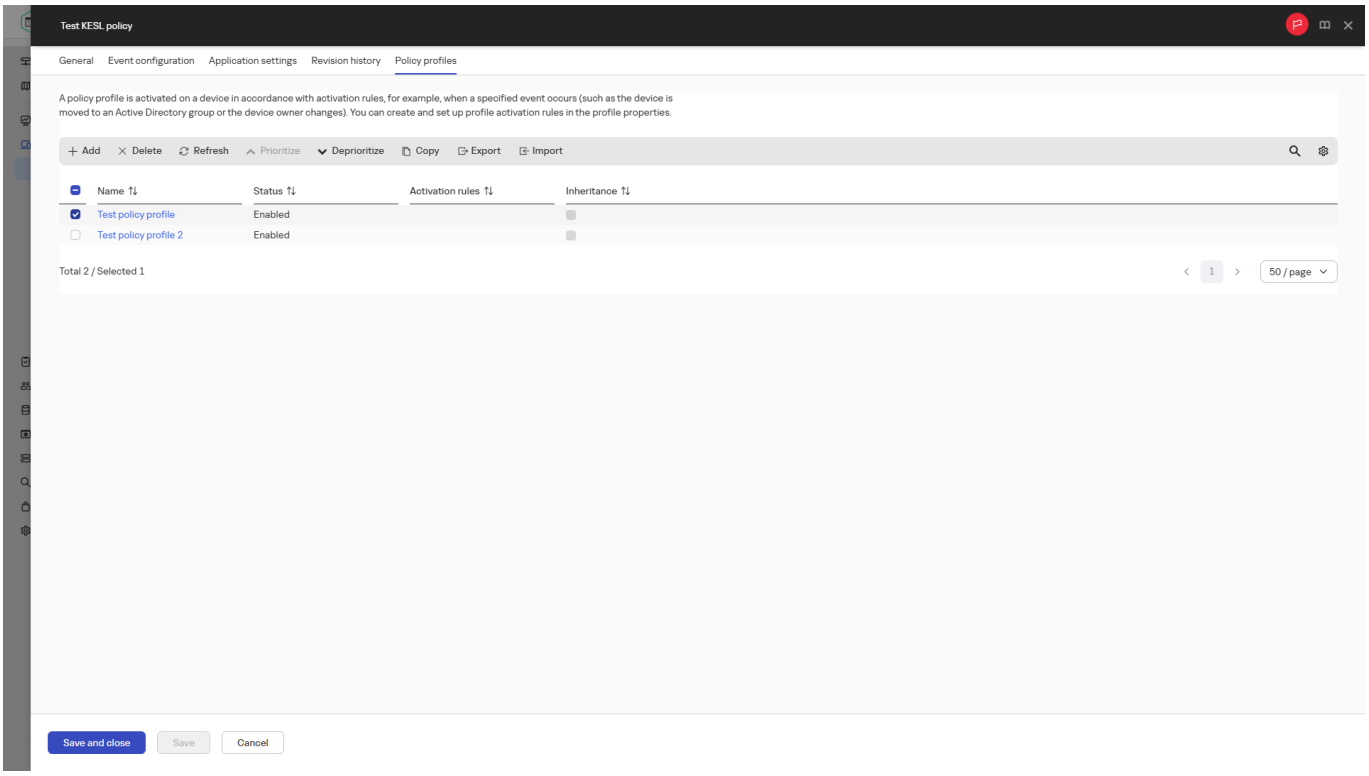
# Changing a policy profile priority

*To change a policy profile priority:*

1. Proceed to the list of profiles of the policy that you want.

   The list of policy profiles appears.
2. On the **Policy profiles** tab, select the check box next to the policy profile for which you want to change priority.
3. Set a new position of the policy profile in the list by clicking **Prioritize** or **Deprioritize**.

   The higher a policy profile is located in the list, the higher its priority.




4. Click the **Save** button.

   Priority of the selected policy profile is changed and applied.

## Creating a policy profile

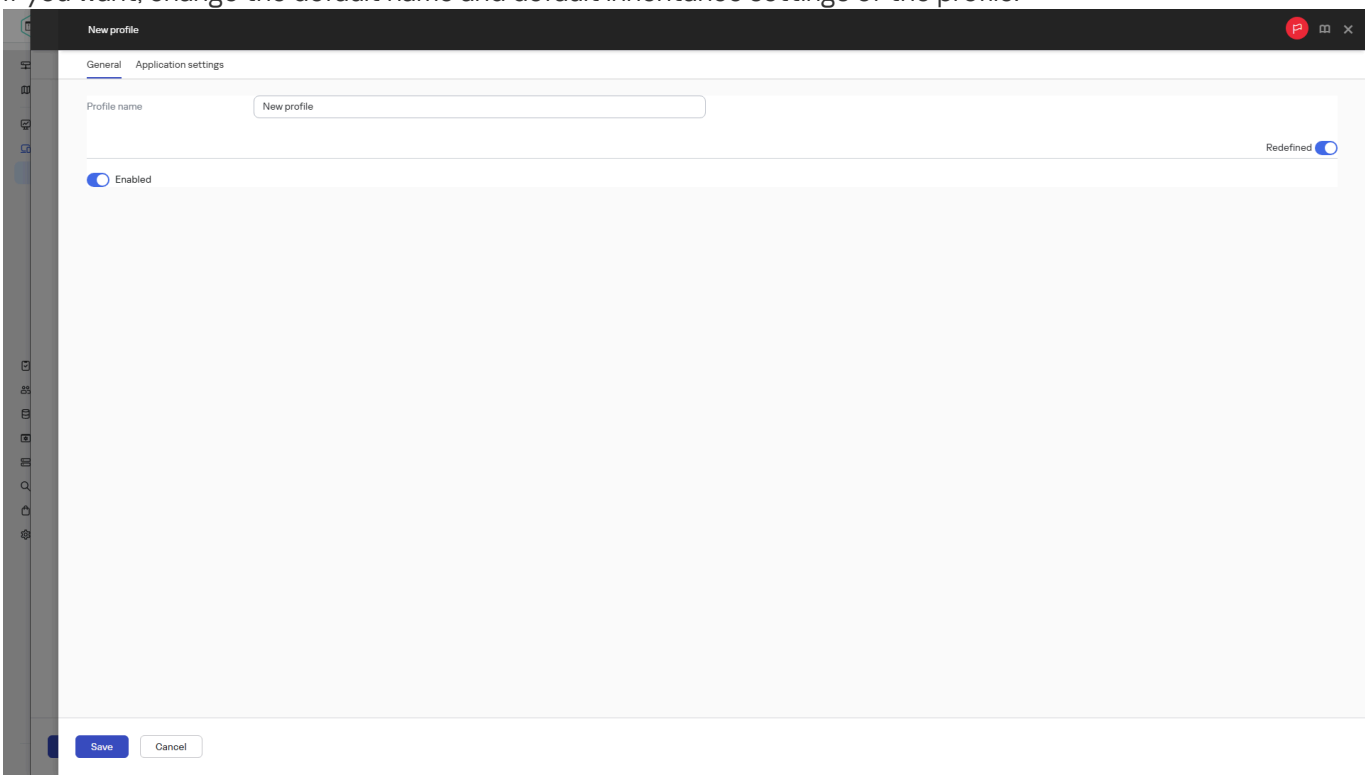
*To create a policy profile:*

1. Proceed to the list of profiles of a policy that you want.

   The list of policy profiles appears. If the policy does not have profiles, an empty table appears.

2. Click **Add**.

3. If you want, change the default name and default inheritance settings of the profile.



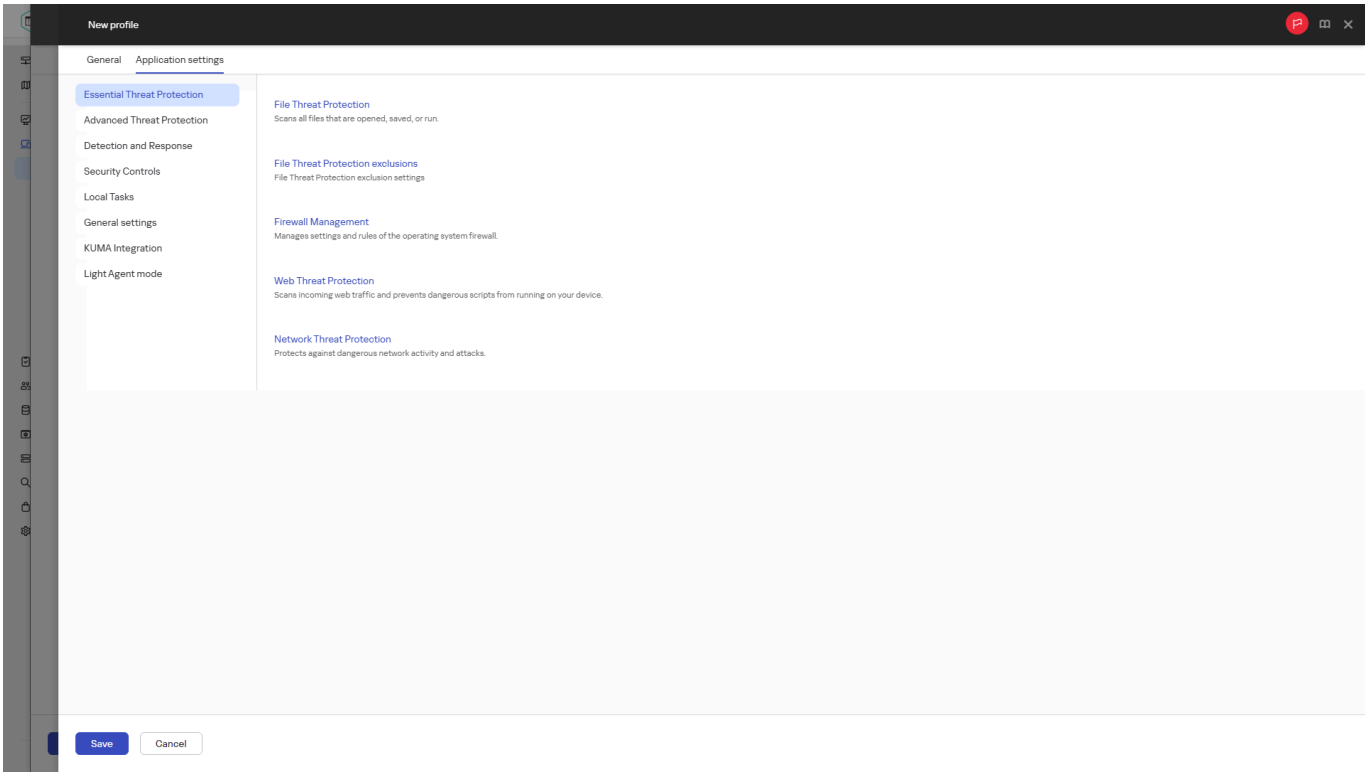

Creating a policy profile

4. Select the **Application settings** tab.

   Alternatively, you can click **Save** and exit. The profile that you have created appears in the list of policy profiles, and you can edit its settings later.

5. On the **Application settings** tab, in the left pane, select the category that you want and in the results pane on the right, edit the settings for the profile. You can edit policy profile settings in each category (section).

When editing the settings, you can click **Cancel** to cancel the last operation.




Specifying the policy profile settings

6. Click **Save** to save the profile.

The profile will appear in the list of policy profiles.

## Copying a policy profile

You can copy a policy profile to the current policy or to another, for example, if you want to have identical profiles for different policies. You can also use copying if you want to have two or more profiles that differ in only a small number of settings.

*To copy a policy profile:*

1. Proceed to the list of profiles of the policy that you want.

   The list of policy profiles appears. If the policy does not have profiles, an empty table appears.

2. On the **Policy profiles** tab, select the policy profile that you want to copy.

3. Click the **Copy** button.

4. In the window that opens, select the policy to which you want to copy the profile.

   You can copy a policy profile to the same policy or to a policy that you specify.

5. Click the **Copy** button.

The policy profile is copied to the policy that you selected. The newly copied profile gets the lowest priority. If you copy the profile to the same policy, the name of the newly copied profile will be expanded with the () index, for example: (1), (2).

You can later change the settings of the policy profile, including its name and priority. In this case, the original policy profile is not changed.

## Creating a policy profile activation rule

*To create a policy profile activation rule:*

1. Proceed to the list of profiles of the policy that you want.

   The list of policy profiles appears.

2. On the **Policy profiles** tab, click the policy profile for which you need to create an activation rule.

   If the list of policy profiles is empty, you can create a policy profile.

3. On the **Activation rules** tab, click the **Add** button.

   The window with policy profile activation rules opens.

4. Specify a name for the rule.

5. Select the check boxes next to the conditions that must affect activation of the policy profile that you are creating:

   **General rules for policy profile activation**

   Select this check box to set up policy profile activation rules on the device depending on the status of the device offline mode, rule for connection to Administration Server, and tags assigned to the device.

   For this option, specify at the next step:

   **Device status**

   Defines the condition for device presence on the network:

   - **Online**—The device is on the network, and so the Administration Server is available.
   - **Offline**—The device is on an external network, which means that the Administration Server is not available.
   - **N/A**—The criterion will not be applied.

   **Network location of the device**

   Choose the condition of policy profile activation (whether the rule is executed or not) and select the rule name.

   The rule defines the network location of the device for connection to the Administration Server, whose conditions must be met (or must not be met) for activation of the policy profile.

   A network location description of devices for connection to an Administration Server can be created or configured in a Network Agent switching rule.

   - **Rules for specific device owner**

     For this option, specify at the next step:

     **Device owner**

Enable this option to configure and enable the rule for profile activation on the device according to its owner. In the drop-down list under the check box, you can select a criterion for the profile activation:

- The device belongs to the specified owner ("=" sign).
- The device does not belong to the specified owner ("#" sign).

  If this option is enabled, the profile is activated on the device in accordance with the criterion configured. You can specify the device owner when the option is enabled. If this option is disabled, the profile activation criterion is not applied. By default, this option is disabled.

**Device owner is included in an internal security group**

Enable this option to configure and enable the rule of profile activation on the device by the owner's membership in an internal security group of Kaspersky Security Center Linux. In the drop-down list under the check box, you can select a criterion for the profile activation:

- The device owner is a member of the specified security group ("=" sign).
- The device owner is not a member of the specified security group ("#" sign).

  If this option is enabled, the profile is activated on the device in accordance with the criterion configured. You can specify a security group of Kaspersky Security Center Linux. If this option is disabled, the profile activation criterion is not applied. By default, this option is disabled.

- **Rules for hardware specifications**

  Select this check box to set up rules for policy profile activation on the device depending on the memory volume and the number of logical processors.

  For this option, specify at the next step:

  **RAM size, in MB**

  Enable this option to configure and enable the rule of profile activation on the device by the RAM volume available on that device. In the drop-down list under the check box, you can select a criterion for the profile activation:

  - The device RAM size is less than the specified value ("<" sign).
  - The device RAM size is greater than the specified value (">" sign).

  If this option is enabled, the profile is activated on the device in accordance with the criterion configured. You can specify the RAM volume on the device. If this option is disabled, the profile activation criterion is not applied. By default, this option is disabled.

  **Number of logical processors**

  Enable this option to configure and enable the rule of profile activation on the device by the number of logical processors on that device. In the drop-down list under the check box, you can select a criterion for the profile activation:

  - The number of logical processors on the device is less than or equal to the specified value ("<" sign).
  - The number of logical processors on the device is greater than or equal to the specified value (">" sign).

  If this option is enabled, the profile is activated on the device in accordance with the criterion configured. You can specify the number of logical processors on the device. If this option is disabled, the profile activation criterion is not applied. By default, this option is disabled.

- **Rules for role assignment**

  For this option, specify at the next step:

**Activate policy profile by specific role of device owner**

Select this option to configure and enable the rule of profile activation on the device depending on the owner's role. Add the role manually from the list of existing roles.

If this option is enabled, the profile is activated on the device in accordance with the criterion configured.

- **Rules for tag usage**

  Select this check box to set up rules for policy profile activation on the device depending on the tags assigned to the device. You can activate the policy profile to the devices that either have the selected tags or do not have them.

  For this option, specify at the next step:

  **Tag list**

  In the list of tags, specify the rule for device inclusion in the policy profile by selecting the check boxes next to the relevant tags.

  You can add new tags to the list by entering them in the field over the list and clicking the **Add** button.

  The policy profile includes devices with descriptions containing all the selected tags. If check boxes are cleared, the criterion is not applied. By default, these check boxes are cleared.

  **Apply to devices without the specified tags**

  Enable this option if you have to invert your selection of tags.

  If this option is enabled, the policy profile includes devices with descriptions that contain none of the selected tags. If this option is disabled, the criterion is not applied.

  By default, this option is disabled.

- **Rules for Active Directory usage**

  Select this check box to set up rules for policy profile activation on the device depending on the presence of the device in an Active Directory organizational unit (OU), or on membership of the device (or its owner) in an Active Directory security group.

  For this option, specify at the next step:

  **Device owner's membership in an Active Directory security group**

  If this option is enabled, the policy profile is activated on the device whose owner is a member of the specified security group. If this option is disabled, the profile activation criterion is not applied. By default, this option is disabled.

  **Device membership in Active Directory security group**

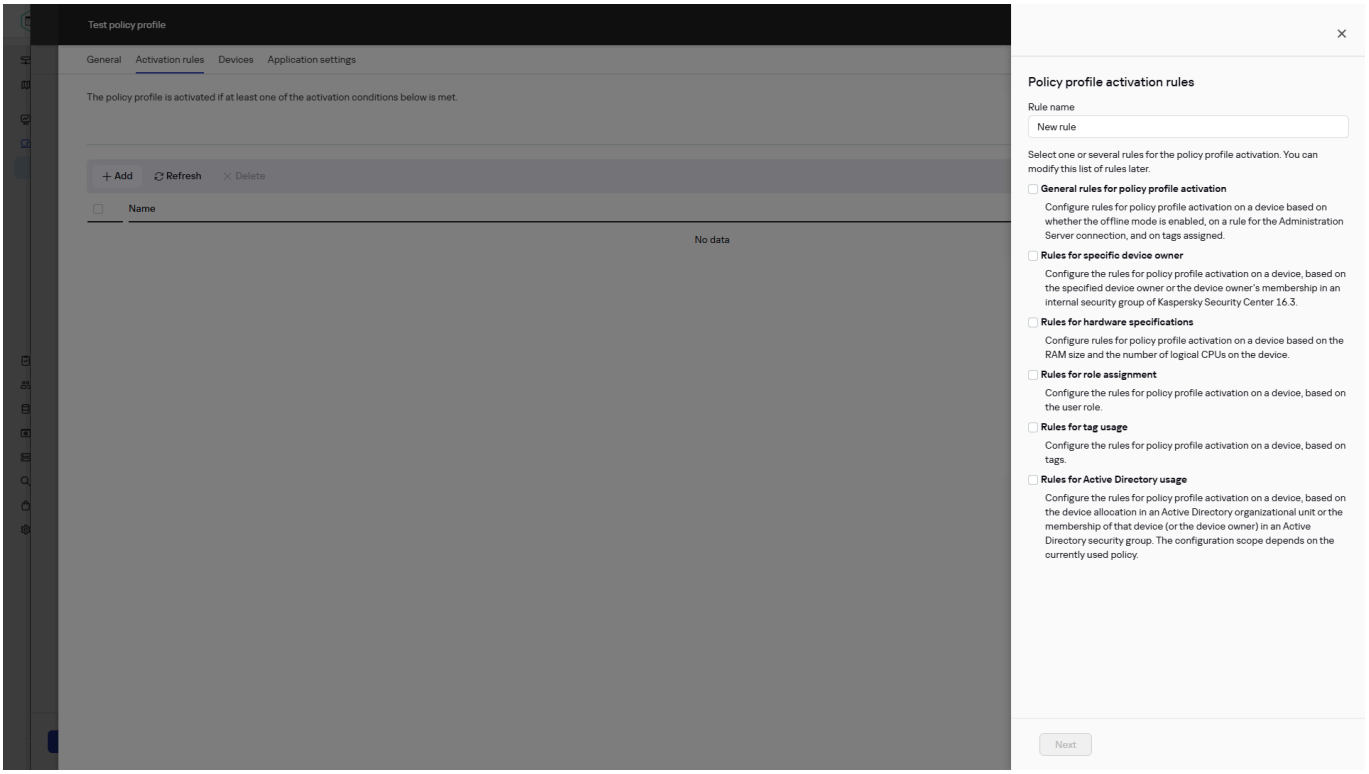
  If this option is enabled, the policy profile is activated on the device. If this option is disabled, the profile activation criterion is not applied. By default, this option is disabled.

  **Device allocation in Active Directory organizational unit**

  If this option is enabled, the policy profile is activated on the device which is included in the specified Active Directory organizational unit (OU). If this option is disabled, the profile activation criterion is not applied.

  By default, this option is disabled.

The number of additional pages of the wizard depends on the settings that you select at the first step. You can modify policy profile activation rules later.




Creating a policy profile activation rule

6. Check the list of the configured parameters. If the list is correct, click **Create**.

   The profile will be saved. The profile will be activated on the device when activation rules are triggered.

Policy profile activation rules created for the profile are displayed in the policy profile properties on the **Activation rules** tab. You can modify or remove any policy profile activation rule.

Multiple activation rules can be triggered simultaneously.

## Deleting a policy profile

*To delete a policy profile:*

1. Proceed to the list of profiles of the policy that you want.

   The list of policy profiles appears.

2. On the **Policy profiles** tab, select the check box next to the policy profile that you want to delete, and click **Delete**.

3. In the window that opens, click **Delete** again.

   The policy profile is deleted. If the policy is inherited by a lower-level group, the profile remains in that group, but becomes the policy profile of that group. This is done to eliminate significant change in settings of the managed applications installed on the devices of lower-level groups.

# Exporting and importing a policy profile

You can save a policy profile to a KLPROF file without exporting a policy, and then use this KLPROF file to import the saved profile to the policy.

This allows you to restore the policy profile settings quickly, instead of configuring them again.

A policy profile is imported to the policy of the same version of the application from which you exported the profile. For applications that support backward compatibility of policies (for example, Kaspersky Endpoint Security for Windows), you can import policy profiles to different versions of the policy.

*To export a policy profile:*

1. Proceed to the list of profiles of a policy that you want.

   The list of policy profiles appears.

2. On the **Policy profiles** tab, click the policy profile that you want to export.

3. In the toolbar, click the **Export** button.

4. In the window that opens, specify the directory to which you want to save the file with the policy profile.

   You can change the file name, if necessary.

5. Click the **Save** button.

If the operation is completed successfully, an appropriate message is displayed on the screen. Otherwise, an error message is displayed.

*To import a policy profile:*

1. Proceed to the list of profiles of the policy that you want.

   The list of policy profiles appears.

2. In the toolbar, click the **Import** button.

3. In the window that opens, select the KLPROF file with the required policy profile, and then click the **Open** button.

   The maximum size of the imported file is 4 MB.

If the operation is completed successfully, an appropriate message is displayed on the screen. Otherwise, an error message is displayed.

The policy profile is imported with the name it had when you exported it, not with the name of the KLPROF file. The file is imported with the **Disabled** status and the lowest priority, regardless of the priority the policy profile had before the export.

You cannot perform the import:

- If the policy already has a profile with the same name.
- If the number of profiles in the policy is 100.

# Network Agent policy settings

*To configure the Network Agent policy:*

1. In the main menu of the application, go to **Asset management** → **Policies**.
2. Click the name of the Network Agent policy.

   The properties window of the Network Agent policy opens. The properties window contains the tabs and settings described below.

See the comparison table detailing how the settings below apply, depending on the type of operating system used.

## General

On this tab, you can modify the policy name, policy status, and specify the inheritance of policy settings:

- In the **Name** field, you can modify the policy name.
- In the **Policy status** block, you can select one of the policy modes:

  **Active**

  If this option is selected, the policy becomes active.

  By default, this option is selected.

  **Inactive**

  If this option is selected, the policy becomes inactive, but it is still stored in the **Policies** folder. If required, the policy can be activated.

- In the **Settings inheritance** settings group, you can configure the policy inheritance:

  **Inherit settings from parent policy**

  If this option is enabled, the policy setting values are inherited from the upper-level group policy and, therefore, are locked.

  By default, the option is enabled.

  **Force inheritance of settings in child policies**

If this option is enabled, after policy changes are applied, the following actions will be performed:

- The values of the policy settings will be propagated to the policies of administration subgroups, that is, to the child policies.
- In the **Settings inheritance** block of the **General** section in the properties window of each child policy, the **Inherit settings from parent policy** option will be automatically enabled.

If this option is enabled, the child policies settings are locked.

By default, this option is disabled.

## Event configuration

On this tab, you can configure event logging and event notification. Events are distributed according to importance level in the following sections:

- **Functional failure**
- **Warning**
- **Info**

In each section, the list shows the types of events and the default event storage period on the Administration Server (in days). After you click the event type, you can specify the settings of event logging and notifications about events selected in the list. By default, common notification settings specified for the entire Administration Server are used for all event types. However, you can change specific settings for the required event types.

For example, in the **Warning** section, you can configure the **Security issue has occurred** event type. Such events may happen, for instance, when the free disk space of a distribution point is less than 2 GB (at least 4 GB are required to install applications and download updates remotely). To configure the **Security issue has occurred** event, click it and specify where to store the occurred events and how to notify about them.

If the Network Agent detects a security issue, you can manage this issue by using the settings of a managed device.

## Application settings

## Settings

In the **Settings** section, you can configure the Network Agent policy:

**Distribute files through distribution points only**

If this option is enabled, Network Agents on managed devices retrieve updates from distribution points only.

If this option is disabled, Network Agents on managed devices retrieve updates from distribution points or from Administration Server.

Note that the security applications on managed devices retrieve updates from the source set in the update task for each security application. If you enable the **Distribute files through distribution points only** option, make sure that Kaspersky Security Center Linux is set as an update source in the update tasks.

By default, this option is disabled.

**Maximum size of event queue, in MB**

In this field you can specify the maximum space on the drive that an event queue can occupy.

The default setting is 2 MB.

**&Application is allowed to retrieve policy's extended data on device**

Network Agent installed on a managed device transfers information about the applied security application policy to the security application (for example, Kaspersky Endpoint Security for Linux). You can view the transferred information in the security application interface.

Network Agent transfers the following information:

- Time of the policy delivery to the managed device.
- Name of the active policy at the moment of the policy delivery to the managed device.
- Name of the out-of-office policy at the moment of the policy delivery to the managed device (not available for the Network Agent for Linux).
- Name and full path to the administration group that contained the managed device at the moment of the policy delivery to the managed device.
- List of active policy profiles with their names and priorities at the moment of the policy delivery to the managed device.

You can use the information to ensure the correct policy is applied to the device and for troubleshooting purposes. By default, this option is disabled.

**Protect the Network Agent service against unauthorized removal or termination, and prevent changes to the settings**

When this option is enabled, after Network Agent is installed on a managed device, the component cannot be removed or reconfigured without required privileges. The Network Agent service cannot be stopped. This option has no effect on domain controllers.

Enable this option to protect Network Agent on workstations operated with local administrator rights.

By default, this option is disabled.

**Use uninstallation password**

If this option is enabled, by clicking the **Modify** button you can specify the password for the klmover utility and Network Agent remote uninstallation on Windows-based devices.

By default, this option is disabled.

## Repositories

In the **Repositories** section, you can select the types of objects whose details will be sent from Network Agent to Administration Server:

**Details of installed applications**

If this option is enabled, information about applications installed on client devices is sent to the Administration Server.

By default, the option is enabled.

**Include information about patches**

Information about patches of applications installed on client devices is sent to the Administration Server. Enabling this option may increase the load on the Administration Server and DBMS, as well as cause increased volume of the database.

By default, the option is enabled. It is available only for Windows.

**Details of Windows Update updates**

If this option is enabled, information about mandatory Microsoft Windows Update updates that must be installed on client devices is sent to the Administration Server.

By default, the option is enabled. It is available only for Windows.

Information about optional Microsoft Windows updates is not being sent to the Administration Server.

**Details of software vulnerabilities and corresponding updates**

If this option is enabled, information about vulnerabilities in third-party software (including Microsoft software), detected on managed devices, and about software updates to fix third-party vulnerabilities (not including Microsoft software) is sent to the Administration Server.

Selecting this option (**Details of software vulnerabilities and corresponding updates**) increases the network load, Administration Server disk load, and Network Agent resource consumption.

By default, the option is enabled. It is available only for Windows.

To manage software updates of Microsoft software, use the **Details of Windows Update updates** option.

**Hardware registry details**

Network Agent installed on a device sends information about the device hardware to the Administration Server. You can view the hardware details in the device properties.

Ensure that the lshw utility is installed on Linux devices from which you want to fetch hardware details. Hardware details fetched from virtual machines may be incomplete depending on the hypervisor used.

If modification of some settings in this section is prohibited by the Network Agent policy, you cannot modify these settings.

## Software updates and vulnerabilities

In the **Software updates and vulnerabilities** section, you can enable scanning of executable files for vulnerabilities:

**Scan executable files for vulnerabilities when running them**

If this option is enabled, executable files are scanned for vulnerabilities when they are run.

By default, the option is enabled.

## Restart management

In the **Restart management** section, you can specify the action to be performed if the operating system of a managed device has to be restarted for correct use, installation, or uninstallation of an application:

**Do not restart the operating system**

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

**Restart the operating system automatically, if necessary**

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

**Prompt user for action**

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

**Repeat the prompt every (min)**

If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

By default, the option is enabled. The default interval is 5 minutes. Available values are between 1 and 1440 minutes.

If this option is disabled, the prompt is displayed only once.

**Force restart after (min)**

After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, the option is enabled. The default delay is 30 minutes. Available values are between 1 and 1440 minutes.

**Force closure of applications in blocked sessions**

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

## Manage patches and updates

In the Manage patches and updates section, you can configure the download and distribution of updates, as well as the installation of patches, on managed devices:

**Automatically install applicable updates and patches for components that have the Undefined status**

If this option is enabled, Kaspersky patches that have the *Undefined* approval status are automatically installed on managed devices immediately after they are downloaded from update servers.

If this option is disabled, Kaspersky patches that have been downloaded and tagged with the *Undefined* status will be installed only after you change their status to *Approved*.

By default, the option is enabled.

**Download updates and anti-virus databases from Administration Server in advance (recommended)**

If this option is enabled, the offline model of update download is used. When the Administration Server receives updates, it notifies Network Agent (on devices where it is installed) of the updates that will be required for managed applications. When Network Agent receives information about these updates, it downloads the relevant files from the Administration Server in advance. At the first connection with Network Agent, the Administration Server initiates an update download. After Network Agent downloads all the updates to a client device, the updates become available for applications on that device.

When a managed application on a client device attempts to access Network Agent for updates, Network Agent checks whether it has all required updates. If the updates are received from the Administration Server not more than 25 hours before they were requested by the managed application, Network Agent does not connect to the Administration Server but supplies the managed application with updates from the local cache instead. Connection with the Administration Server may not be established when Network Agent provides updates to applications on client devices, but connection is not required for updating.

If this option is disabled, the offline model of update download is not used. Updates are distributed according to the schedule of the update download task.

By default, the option is enabled.

## Connectivity

The **Connectivity** section includes three subsections:

- **Network**
- **Connection profiles**
- **Connection schedule**

In the **Network** subsection, you can configure the connection to Administration Server, enable the use of a UDP port, and specify the UDP port number.

- In the **Connect to Administration Server** settings group, you can configure connection to the Administration Server and specify the time interval for synchronization between client devices and the Administration Server:

  **Synchronization interval (min)**

  Network Agent synchronizes the managed device with the Administration Server. We recommend that you set the synchronization interval (also referred to as the heartbeat) to 15 minutes per 10,000 managed devices.

  **Compress network traffic**

  If this option is enabled, the speed of data transfer by Network Agent is increased by means of a decrease in the amount of information being transferred and a consequent decreased load on the Administration Server.

  > The workload on the CPU of the client computer may increase.

  By default, this check box is enabled.

  **Open Network Agent ports in Microsoft Windows Firewall**

  If this option is enabled, the ports, necessary for the work of Network Agent, are added to the Microsoft Windows Firewall exclusion list.

  By default, the option is enabled.

  **Use SSL connection**

  If this option is enabled, connection to the Administration Server is established through a secure port via SSL.

  By default, the option is enabled.

  **Use the connection gateway on a distribution point (if available), under the default connection settings**

  If this option is enabled, the connection gateway on the distribution point is used under the settings specified in the administration group properties.

  By default, the option is enabled.

- **Use UDP port**

  If you need Network Agent to connect to Administration Server through a UDP port, enable the **Use UDP port** option and specify a **UDP port number**. By default, the option is enabled. The default UDP port to connect to Administration Server is 15000.

- **UDP port number**

  In this field you can enter the UDP port number. The default port number is 15000.

  The decimal system is used for records.

- **Use distribution point to force connection to Administration Server**

  Select this option if you selected the **Use this distribution point as a push server** option in the distribution point settings window. Otherwise, the distribution point will not act as a push server.

In the **Connection profiles** subsection, you can specify the network location settings and enable out-of-office mode when Administration Server is not available:

**Network location settings**

Network location settings define the characteristics of the network to which the client device is connected and specify rules for Network Agent switching from one Administration Server connection profile to another when those network characteristics are altered.

**Administration Server connection profiles**

You can view and add profiles for Network Agent connection to the Administration Server. In this section, you can also create rules for switching Network Agent to different Administration Servers when the following events occur:

- When the client device connects to a different local network
- When the device loses connection with the local network of the organization
- When the connection gateway address is changed or the DNS server address is modified

**Enable out-of-office mode when Administration Server is not available**

If this option is enabled, in case of connection through this profile, applications installed on the client device use policy profiles for devices in out-of-office mode, as well as out-of-office policies. If no out-of-office policy has been defined for the application, the active policy will be used.

If this option is disabled, applications will use active policies.

By default, this option is disabled.

In the **Connection schedule** subsection, you can specify the time intervals during which Network Agent sends data to the Administration Server:

**Connect when necessary**

If this option is selected, the connection is established when Network Agent has to send data to the Administration Server.

By default, this option is selected.

**Connect at specified time intervals**

If this option is selected, Network Agent connects to the Administration Server at a specified time. You can add several connection time periods.

## Network polling by distribution points

In the **Network polling by distribution points** section, you can configure automatic polling of the network. You can use the following options to enable the polling and set its frequency:

**Windows network**

The option is available only for Windows-based distribution points.

If the option is enabled, the Administration Server automatically polls the network according to the schedule that you configured by clicking the **Set quick polling schedule** and **Set full polling schedule** links.

If this option is disabled, the Administration Server polls the network with the interval specified in the **Frequency of network polls (min)** field.

The device discovery interval for Network Agent versions can be configured in the **Frequency of polls from Windows domains (min)** (for quick Windows network poll) and **Frequency of network polls (min)** (for full Windows network poll) fields.

By default, this option is disabled.

**IP ranges**

If the option is enabled, the distribution point automatically polls IP ranges according to the schedule that you configured by clicking the **Set polling schedule** button.

If this option is disabled, the distribution point does not poll IP ranges.

The frequency of IP range polling for Network Agent versions prior to 10.2 can be configured in the **Poll interval (min)** field. The field is available if the option is enabled.

By default, this option is disabled.

**Zeroconf**

If this option is enabled, the distribution point automatically polls the network with IPv6 devices by using zero-configuration networking (also referred to as *Zeroconf*). In this case, the enabled IP range polling is ignored, because the distribution point polls the whole network.

To start to use Zeroconf, the following conditions must be fulfilled:

- The distribution point must run Linux.
- You must install the avahi-browse utility on the distribution point.

If this option is disabled, the distribution point does not poll networks with IPv6 devices.

By default, this option is disabled.

**Domain controllers**

If the option is enabled, the distribution point automatically polls domain controllers according to the schedule that you configured by clicking the **Set polling schedule** button.

If this option is disabled, the distribution point does not poll domain controllers.

The frequency of domain controller polling for Network Agent versions prior to 10.2 can be configured in the **Poll interval (min)** field. The field is available if this option is enabled.

By default, this option is disabled.

## Network settings for distribution points

In the **Network settings for distribution points** section, you can specify the internet access settings:

- **Use proxy server**

  If this option is enabled, an internet proxy server is used to connect distribution points to Kaspersky update servers.

- **Address**
- **Port number**
- **Bypass proxy server for local addresses**

  If this option is enabled, no proxy server is used to connect to devices on the local network.

  By default, this option is disabled.

- **Proxy server authentication**

  If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

  This check box is cleared by default.

## KSN Proxy (distribution points)

In the **KSN Proxy (distribution points)** section, you can configure the application to use the distribution point to forward Kaspersky Security Network (KSN) requests from the managed devices:

**Enable KSN Proxy on the distribution point side**

The KSN proxy service is run on the device that is used as a distribution point. Use this feature to redistribute and optimize traffic on the network.

The distribution point sends the KSN statistics, which are listed in the Kaspersky Security Network statement, to Kaspersky.

By default, this option is disabled. Enabling this option takes effect only if the **Use Administration Server as a proxy server** and **I agree to use Kaspersky Security Network** options are enabled in the Administration Server properties window.

You can assign a node of an active-passive cluster to a distribution point and enable KSN proxy server on this node.

**Forward KSN requests to Administration Server**

The distribution point forwards KSN requests from the managed devices to the Administration Server.

By default, the option is enabled.

**Access KSN Cloud/KPSN directly over the internet**

The distribution point forwards KSN requests from managed devices to the KSN Cloud or KPSN. The KSN requests generated on the distribution point itself are also sent directly to the KSN Cloud or KPSN.

**TCP port**

The number of the TCP port that the managed devices will use to connect to KSN proxy server. The default port number is 13111.

**UDP port**

If you need Network Agent to connect to Administration Server through a UDP port, enable the **Use UDP port** option and specify a **UDP port number**. By default, the option is enabled. The default UDP port to connect to Administration Server is 15000.

**HTTPS port**

If you need the managed devices to connect to the KSN proxy server through an HTTPS port, enable the **Use HTTPS** option, and then specify a port number in the **HTTPS port** field. By default, this option is disabled. The default HTTPS port to connect to the KSN proxy server is 17111.

## Updates (distribution points)

In the **Updates (distribution points)** section, you can enable the downloading diff files feature, so distribution points take updates in the form of diff files from Kaspersky update servers.

## Local account management (Linux only)

The **Local account management (Linux only)** section includes three subsections:

- **User certificates management**
- **Add or edit applicable local administrator groups**
- **Upload a reference file to protect the sudoers file on the user's device from changes**

In the **User certificates management** subsection, you can specify which root certificates to install. These certificates can be used, for example, to verify the authenticity of websites or web servers.

**Install root certificates**

If this option is enabled, certificates added to the table will be installed on the specified devices.

If this option is disabled, no certificates will be installed on the specified devices.

By default, this option is disabled.

**Add**

Clicking this button opens a window, in which where you can add a certificate.

The certificate must be less than 10 MB.

Kaspersky Security Center supports certificates with CER, CRT, CERT, PEM, and KEY extensions.

In the **Add or edit applicable local administrator groups** subsection, you can manage local administrator groups. These groups are used, for example, when revoking local administrator rights. You can also check the list of privileged user accounts using the **Report on privileged device users (Linux only)**.

**Add**

Clicking this button opens a window, where you can add a local administrator group.

**Edit**

Clicking this button opens a window, where you can edit the local administrator group.

This button is available if the check box next to the local administrator group is selected.

**Delete**

Clicking this button deletes the selected local administrator group from the table.

This button is available if the check box next to the local administrator group is selected.

In the **Upload a reference file to protect the sudoers file on the user's device from changes** subsection, you can configure control of the sudoers file. Privileged groups and device users are defined by the sudoers file on the device. The sudoers file is located at `/etc/sudoers`. You can upload a reference sudoers file to protect the sudoers file from changes. This will prevent unwanted changes to the sudoers file.

An invalid reference sudoers file may cause the user's device to malfunction.

**Control sudoers file**

If this option is enabled, the sudoers file will be replaced by the current reference sudoers file.

If this option is disabled, the sudoers file will remain unchanged.

By default, this option is disabled.

**Reference sudoers file**

This field displays the name of the uploaded reference sudoers file.

**Upload**

Clicking this button opens a window, where you can upload a reference sudoers file.

**Current reference sudoers file**

Clicking this button shows the contents of the current sudoers file.

### Revision history

On the **Revision history** tab, you can:

- View and save the history of policy revisions.
- Roll back to a policy revision.
- Add and edit policy revision descriptions.
- Compare policy revisions.

# Usage of Network Agent for Windows, Linux, and macOS: Comparison

The Network Agent usage varies depending on the operating system of the device. The Network Agent policy and installation package settings also differ depending on the operating system. The table below compares Network Agent features and usage scenarios available for Windows, Linux, and macOS operating systems.

| Network Agent feature | Windows | Linux | macOS |
|---|---|---|---|
| **Installation** | | | |
| Installing by cloning an image of the administrator's hard drive with the operating system and Network Agent using third-party tools | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | ✓ | ✓ |
| Installing with third-party tools for remote installation of applications | ✓ | ✓ | ✓ |
| Installing manually, by running application installers on devices | ✓ | ✓ | ✓ |
| Installing Network Agent in silent mode | ✓ | ✓ | ✓ |
| Manually connecting a client device to the Administration Server. klmover utility | ✓ | ✓ | ✓ |
| Automatic installing of updates and patches for Kaspersky Security Center components | ✓ | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | – |
| Automatic distributing of a key | ✓ | ✓ | ✓ |
| Forced synchronization | ✓ | ✓ | ✓<br>Except a push server |
| **Distribution point** | | | |
| Using as distribution point | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | ✓ |
| Calculating the number and configuration of distribution points | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | ✓<br>Without using Network Location Awareness (NLA).<br>Limitation: not supported by Network Agent Elbrus Edition. | ✓<br>Without using Network Location Awareness (NLA). |
| Offline model of update download | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | ✓ |
| Network polling | ✓<br>• IP range polling<br>• Domain controller polling (Microsoft Active Directory)<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | ✓<br>IP range polling<br>Zeroconf polling<br>Domain controller polling (Microsoft Active Directory, Samba 4 Active Directory, FreeIPA, ALD Pro)<br>Limitation: not supported by Network Agent Elbrus Edition. | – |

| Network Agent feature | Windows | Linux | macOS |
|---|---|---|---|
| Running KSN proxy service on a distribution point side | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | – |
| Downloading updates via Kaspersky update servers to the distribution points repositories that distribute updates to managed devices | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | –<br>(If one or more devices running Linux or macOS are within the scope of the Download updates to the repositories of distribution points task, the task completes with the Failed status, even if it has successfully completed on all Windows devices.) |
| Push installation of applications | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | Restricted: it is not possible to perform push installation on Windows devices by using Linux distribution points. Not supported by Network Agent Elbrus Edition. | Restricted: it is not possible to perform push installation on Windows devices by using macOS distribution points. |
| Using as a push server | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | – |
| **Handling third-party applications** | | | |
| Remote installing of applications on devices | ✓ | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | ✓<br>Refer to the following article for details: Remote installing of applications on macOS devices. |
| Configuring operating system updates in a Network Agent policy | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | – | – |
| Viewing information about software vulnerabilities | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | – | – |
| Scanning applications for vulnerabilities | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | – | – |
| Software updates | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | – | – |
| Inventory of software installed on devices | ✓ | ✓ | – |
| **Virtual machines** | | | |
| Installing Network Agent on a virtual machine | ✓ | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | ✓ |

| Network Agent feature | Windows | Linux | macOS |
| --- | --- | --- | --- |
| Optimization settings for virtual desktop infrastructure (VDI) | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | ✓ |
| Support of dynamic virtual machines | ✓<br>Limitation: Not supported by Network Agent for Microsoft Windows on Arm. | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | ✓ |
| **Other** | | | |
| Auditing actions on a remote client device by using Windows Desktop Sharing | ✓ | — | — |
| Monitoring the anti-virus protection status | ✓ | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | ✓ |
| Managing device restarts | ✓ | — | — |
| Support of file system rollback | ✓ | ✓ | ✓ |
| Using a Network Agent as connection gateway | ✓ | ✓ | ✓ |
| Connection Manager | ✓ | ✓ | ✓ |
| Connection profiles for out-of-office users | ✓ | ✓ | ✓ |
| Network Agent switching from one Administration Server to another (automatically by network location) | ✓ | ✓ | ✓ |
| Checking the connection between a client device and the Administration Server. Klnagchk utility | ✓ | ✓ | ✓ |
| Remotely connecting to the desktop of a client device | ✓ | ✓<br>Limitation: not supported by Network Agent Elbrus Edition. | ✓<br>By using the Virtual Network Computing (VNC) system. |
| Downloading a stand-alone installation package through the Migration wizard | ✓ | ✓ | ✓ |
| Viewing information about the hardware of client devices | ✓ | ✓<br>Information about the hardware of Linux devices sent to the Administration Server by Network Agent installed on these devices is limited to the information specified in the description of the managed device settings. | ✓<br>Information about the hardware of macOS devices sent to the Administration Server by Network Agent installed on these devices is limited to the information specified in the description of the managed device settings. |

# Comparison of Network Agent settings by operating systems

The table below shows which Network Agent policy settings are available depending on the operating system of the managed device where Network Agent was installed.

Network Agent settings: comparison by operating systems

| Settings section | Windows | Linux | macOS |
|---|---|---|---|
| General | ✓ | ✓ | ✓ |
| Event configuration | ✓ | ✓ | ✓ |
| Settings | ✓ | ✓<br>The following options are available:<br>• **Distribute files through distribution points only**<br>• **Maximum size of event queue, in MB**<br>• **&Application is allowed to retrieve policy's extended data on device** | ✓ |
| Repositories | ✓ | ✓<br>The following options are available:<br>• **Details of installed applications**<br>• **Hardware registry details** | ✓<br>The **Hardware registry details** option is available. |
| Connectivity → Network | ✓ | ✓<br>Except the **Open Network Agent ports in Microsoft Windows Firewall** option. | ✓ |
| Connectivity → Connection profiles | ✓ | ✓ | ✓ |
| Connectivity → Connection schedule | ✓ | ✓ | ✓ |
| Network polling by distribution points | ✓<br>The following settings are available:<br>• **Windows network**<br>• **IP ranges**<br>• **Domain controllers** | ✓<br>The following settings are available:<br>• **Zeroconf**<br>• **IP ranges**<br>• **Domain controllers** | — |
| Network settings for distribution points | ✓ | ✓ | ✓ |
| KSN Proxy (distribution points) | ✓ | ✓ | — |
| Updates (distribution points) | ✓ | ✓ | — |
| Revision history | ✓ | ✓ | ✓ |

# Enabling and disabling the low resource consumption mode for Network Agent

The low resource consumption mode allows you to limit the RAM usage of the Network Agent installed on the client device. By default, the low resource consumption mode is disabled.

In the low resource consumption mode, the following functions are not performed:

- Network Agent cannot be assigned to act as a distribution point (either manually or automatically).
- Network Agent does not log information about the status of the Network Agent in a separate text file.
- Network Agent does not support the offline model of update download.
- The following components and processes are disabled:
  - Obtaining information about third-party updates and vulnerabilities.
  - Running the KSN Proxy on the distribution point side.
  - Uploading updates to the distribution point repository.
  - Bypassing the DNS server block.
  - Obtaining information about free disk space.

Components and processes resume operation after disabling the low resource consumption mode.

*To enable the low resource consumption mode:*

1. Execute the following command in the command line on the client device:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Restart the Network Agent by using the following command:

   ```
   sudo service klnagent64 restart
   ```

3. In the operating system log, check if the **Kaspersky Security Center Network Agent is working in low resource consumption mode** entry is displayed.

The low resource consumption mode is enabled.

*To disable the low resource consumption mode:*

1. Execute the following command in the command line on the client device:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Restart the Network Agent by using the following command:

   ```
   sudo service klnagent64 restart
   ```

The low resource consumption mode is disabled.

You can also enable the low resource consumption mode remotely by using an *Execute scripts remotely* task.

# Configuring protection settings of managed applications

To configure the protection settings of managed Kaspersky applications, you can use policies.

For more information about configuring policies of Kaspersky Endpoint Security, see the corresponding Help:

- Kaspersky Endpoint Security for Windows Help
- Kaspersky Endpoint Security for Linux Help
- Kaspersky Endpoint Security for Mac Help

# Manual setup of the group update task for Kaspersky Endpoint Security

The optimal and recommended schedule option for Kaspersky Endpoint Security is **When new updates are downloaded to the repository** when the **Use automatically randomized delay for task starts** check box is selected.

# Manual setup of the group task for scanning a device with Kaspersky Endpoint Security

The quick start wizard creates a group task for scanning a device. If the automatically specified schedule of the group scanning task is not appropriate for your organization, you must manually set up the most convenient schedule for this task based on the workplace rules adopted in the organization.

For example, the task is assigned a **Run on Fridays at 7:00 PM** schedule with automatic randomization, and the **Run missed tasks** check box is cleared. This means that if the devices in the organization are shut down on Fridays, for example, at 6:30 PM, the device scan task will never run. In this case you need to set up the group scanning task manually.

# Kaspersky Security Network (KSN)

This section describes how to use an online service infrastructure named Kaspersky Security Network (KSN). The section provides the details on KSN, as well as instructions on how to enable KSN, configure access to KSN, and view the statistics of the use of KSN proxy server.

Updates functionality (including providing anti-virus signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

# About KSN

Kaspersky Security Network (KSN) is an online service infrastructure that provides access to the online Knowledge Base of Kaspersky, which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the effectiveness of some protection components, and reduces the risk of false positives. KSN allows you to use Kaspersky reputation databases to retrieve information about applications installed on managed devices.

By participating in the Kaspersky Security Network, you agree to automatically provide Kaspersky with information about the operation of security applications installed on computers and mobile devices that are managed using the Kaspersky Security Center Linux. Information is transferred in accordance with the current KSN access settings.

Kaspersky Security Center Linux supports the following KSN infrastructure solutions:

- *Global KSN* is a solution that allows you to exchange information with Kaspersky Security Network. By participating in KSN, you agree to send to Kaspersky in automatic mode information about the operation of Kaspersky applications installed on client devices that are managed through Kaspersky Security Center Linux. Information is transferred in accordance with the current KSN access settings. Kaspersky analysts additionally analyze received information, and include it in the reputation and statistical databases of Kaspersky Security Network. Kaspersky Security Center Linux uses this solution by default.

- *Kaspersky Private Security Network (KPSN)* is a solution that allows users of devices with Kaspersky applications installed to obtain access to reputation databases of Kaspersky Security Network, and other statistical data, without sending data to Global KSN from their own devices. KPSN is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:

  - User devices are not connected to the internet.

  - Transmission of any data outside the country or the corporate LAN is prohibited by law or corporate security policies.

  You can set up access settings of Kaspersky Private Security Network in the **KSN Proxy** section of the Administration Server properties window.

The application prompts you to join KSN while running the Quick Start Wizard. You can start or stop using KSN at any moment when using the application.

You use KSN in accordance with the KSN Statement that you read and accept when you enable KSN. If the KSN Statement is updated, it is displayed to you when you upgrade a version of Administration Server. You can accept the updated KSN Statement or decline it. If you decline it, you keep using KSN in accordance with the previous version of KSN Statement that you accepted before.

When KSN is enabled, Kaspersky Security Center Linux checks if the KSN servers are accessible to make sure the level of security is maintained for the managed devices. If access to the servers using system DNS is not possible, the application uses public DNS servers.

Client devices managed by the Administration Server interact with KSN through KSN proxy server. KSN proxy server provides the following features:

- Client devices can send requests to KSN, obtain information from KSN, and transfer information to KSN even if they do not have direct access to the internet.
- The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

You can configure the KSN proxy server in the **KSN Proxy** section of the Administration Server properties window.

# Setting up access to KSN

You can configure access to Kaspersky Security Network (KSN) from the Administration Server properties, from the Administration Server policy, and from the distribution point.

*To configure the access of the Administration Server to KSN from the Administration Server properties:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **KSN Proxy** section.

3. Set the **Enable KSN Proxy on the Administration Server** toggle switch to Enabled.

   If this option is enabled, KSN proxy server sends data to KSN to increase the efficiency of Kaspersky Security Center components and improve the performance of the Kaspersky applications. Data is sent from client devices to KSN in accordance with the Kaspersky Endpoint Security policy, which is active on those client devices. If this toggle button is disabled, no data will be sent to KSN from the Administration Server and client devices through Kaspersky Security Center Linux. However, client devices can send data to KSN directly (bypassing Kaspersky Security Center Linux), in accordance with their respective settings. The Kaspersky Endpoint Security policy, which is active on client devices, determines which data will be sent directly (bypassing Kaspersky Security Center Linux) from those devices to KSN.

4. Select the KSN infrastructure solution.

   In **Participation in KSN** subsection, do one of the following:

   - If you are using Global KSN, set the toggle switch to the **Use Kaspersky Security Network to Enabled**.

     When enabling this option, make sure to read and accept the terms of the KSN Statement.

   - If you are using KPSN, set the **Use Kaspersky Private Security Network** toggle switch to Enabled and click the **Select file with KSN Proxy settings** button to upload KPSN settings (files with the .pkcs7 and .pem extensions). After the settings are downloaded, the interface displays the provider's name and contacts, as well as the creation date of the file with the settings of KPSN.

   When you set the **Use Kaspersky Private Security Network** toggle switch to Enabled, a message with detailed information about KPSN is dislpayed.

The following Kaspersky applications support KPSN:

- Kaspersky Security Center Linux
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

If you enable KPSN in Kaspersky Security Center Linux, these applications receive information about supporting KPSN. In the settings window of the application, in the **Kaspersky Security Network** subsection of the **Advanced Threat Protection** section, the information about selected KSN provider is displayed — KSN or KPSN.

Kaspersky Security Center Linux does not send any statistical data to Kaspersky Security Network if KPSN is configured in the **KSN Proxy** section of the Administration Server properties window.

5. If you have the proxy server settings configured in the Administration Server properties, but your network architecture requires that you use KPSN directly, enable the **Ignore proxy server settings when connecting to KPSN** option. Otherwise, requests from the managed applications cannot reach KPSN.

6. Configure the Administration Server connection to the KSN proxy service:

   - Under **Connection**, for the **TCP port**, specify the number of the TCP port that will be used for connecting to the KSN proxy server. The default port to connect to the KSN proxy server is 13111.
   - If you want the Administration Server to connect to the KSN proxy server through a UDP port, enable the **Use UDP port** option and specify a port number for the **UDP port**. By default, this option is disabled, and TCP port is used. If this option is enabled, the default UDP port to connect to the KSN proxy server is 15111.
   - If you want the Administration Server to connect to the KSN proxy server through an HTTPS port, enable the **Use HTTPS** option and specify a port number for the **HTTPS port**. By default, this option is disabled, and TCP port is used. If this option is enabled, the default HTTPS port to connect to the KSN proxy server is 17111.

     If you select this option, enable HTTPS on all distribution points that act as a KSN proxy. This avoids overloading the proxy.

7. Enable the **Connect secondary Administration Servers to KSN through the primary Administration Server** toggle switch.

   If this option is enabled, secondary Administration Servers use the primary Administration Server as the KSN proxy server. If this option is disabled, secondary Administration Servers connect to KSN on their own. In this case, managed devices use secondary Administration Servers as KSN proxy servers.

   Secondary Administration Servers use the primary Administration Server as a proxy server if in the right pane of the **KSN Proxy** section, in the properties of secondary Administration Servers, the **Enable KSN Proxy on Administration Server** toggle switch is set to Enabled as well.

8. Click the **Save** button.

The KSN access settings are saved.

*To configure the access of the Administration Server to KSN from the Administration Server policy:*

1. In the main menu, go to **Asset management** → **Policies**.
2. Select an Administration Server policy.
3. In the opened properties window, click the **Application settings** tab.
4. Select the **KSN Proxy** section and follow steps 3 through 8 of the instructions above.

The KSN access settings are saved.

You can also set up distribution point access to KSN, for example, if you want to reduce the load on the Administration Server. The distribution point that acts as a KSN proxy server sends KSN requests from managed devices to Kaspersky directly, without using the Administration Server.

*To set up distribution point access to Kaspersky Security Network (KSN):*

1. Make sure that the distribution point is assigned manually.
2. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.
3. On the **General** tab, select the **Distribution points** section.
4. Click the name of the distribution point to open its properties window.
5. In the distribution point properties window, in the **KSN Proxy** section, enable the **Enable KSN Proxy on the distribution point side** option, and then enable the **Access KSN Cloud/KPSN directly over the internet** option.
6. Click **OK**.

The distribution point will act as a KSN proxy server.

Please note that the distribution point does not support managed device authentication by using the NTLM protocol.

# Enabling and disabling the usage of KSN

*To enable the usage of KSN:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.
2. On the **General** tab, select the **KSN Proxy** section.
3. Set the **Enable KSN Proxy on the Administration Server** toggle switch to Enabled.

The KSN proxy server is enabled and sends data to KSN to increase the efficiency of Kaspersky Next XDR Expert components and improve the performance of Kaspersky applications.

1. Depending on the KSN infrastructure solution that you are using, enable the corresponding toggle buttons.

   - If you are using Global KSN, set the toggle switch to the **Use Kaspersky Security Network to Enabled**.

     Sending data to KSN is now available. When enabling this option, you have to read and accept the terms of the KSN Statement.

   - If you are using KPSN, set the **Use Kaspersky Private Security Network** toggle switch to Enabled and click the **Select file with KSN Proxy settings** button to upload KPSN settings (files with the .pkcs7 and .pem extensions). After the settings are downloaded, the interface displays the provider's name and contacts, as well as the creation date of the file with the settings of KPSN.

     When you set the **Use Kaspersky Private Security Network** toggle switch to Enabled, a message with detailed information about KPSN is dislpayed.

2. Click the **Save** button.

*To disable the usage of KSN:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **KSN Proxy** section.

3. Set the **Enable KSN Proxy on the Administration Server** toggle switch to Disabled to disable the KSN Proxy service.

4. Click the **Save** button.

# Viewing the accepted KSN Statement

When you enable Kaspersky Security Network (KSN), you must read and accept the KSN Statement. You can view the accepted KSN Statement at any time.

*To view the accepted KSN Statement:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **KSN Proxy** section.

3. Click the **View Kaspersky Security Network Statement** link.

In the window that opens, you can view the text of the accepted KSN Statement.

# Accepting an updated KSN Statement

You use KSN in accordance with the KSN Statement that you read and accept when you enable KSN. If the KSN Statement is updated, it is displayed to you when you upgrade a version of Administration Server. You can accept the updated KSN Statement or decline it. If you decline it, you will continue using KSN in accordance with the version of the KSN Statement that you previously accepted.

After upgrading a version of Administration Server, the updated KSN Statement is displayed automatically. If you decline the updated KSN Statement, you can still view and accept it later.

*To view and then accept or decline an updated KSN Statement:*

1. Click the **View notifications** link in the upper-right corner of the main application window.

   The **Notifications** window opens.

2. Click the **View the updated KSN Statement** link.

   The **Kaspersky Security Network Statement update** window opens.

3. Read the KSN Statement, and then make your decision by clicking one of the following buttons:

   - **I accept the updated KSN Statement**
   - **Use KSN under the old Statement**

   Depending on your choice, KSN keeps working in accordance with the terms of the current or updated KSN Statement. You can view the text of the accepted KSN Statement in the properties of Administration Server at any time.

# Checking whether the distribution point works as KSN proxy server

On a managed device assigned to work as a distribution point, you can enable Kaspersky Security Network (KSN) Proxy. A managed device works as the KSN proxy server when the ksnproxy service is running on the device. You can check, turn on, or turn off this service on the device locally.

You can assign a Windows-based or a Linux-based device as a distribution point. The method of distribution point checking depends on the operating system of this distribution point.

*To check whether the Linux-based distribution point works as KSN proxy server:*

1. On the distribution point device, run the `ps aux` command to display the list of running processes.
2. In the list of running processes, check whether the `/opt/kaspersky/klnagent64/sbin/ksnproxy` process is running.

If `/opt/kaspersky/klnagent64/sbin/ksnproxy` process is running, then Network Agent on the device participates in Kaspersky Security Network and works as the KSN proxy server for the managed devices included in the scope of the distribution point.

*To check whether the Windows-based distribution point works as KSN proxy server:*

1. On the distribution point device, in Windows, open **Services** (**All Programs** → **Administrative Tools** → **Services**).

2. In the list of services, check whether the ksnproxy service is running.

   If the ksnproxy service is running, then Network Agent on the device participates in Kaspersky Security Network and works as KSN proxy server for the managed devices included in the scope of the distribution point.

If you want, you may turn off the ksnproxy service. In this case, Network Agent on the distribution point stops participating in Kaspersky Security Network. This requires local administrator rights.

# Viewing the statistics of KSN proxy server

Kaspersky Security Center Web Console allows you to view usage statistics of KSN proxy server.

Statistics includes the following parameters:

- Connection status to KSN
- Number of cache records
- Number of packages processed in cache
- Number of received packages

If you use KPSN as an infrastructure solution, usage statistics of KPSN will be displayed.

*To view the statistics:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **KSN Proxy** section, and then open the **Statistics** tab.

   This tab displays the actual statistics of the use of the KSN proxy server. Statistics refreshes every 15 seconds.

You can copy statistics by clicking the **Copy to clipboard** button.

# Managing tasks

This section describes tasks used by Kaspersky Security Center Linux.

# About tasks

Kaspersky Security Center Linux manages Kaspersky security applications installed on devices by creating and running *tasks*. Tasks are required for installing, launching, and stopping applications, scanning files, updating databases and software modules, and performing other actions on applications.

Tasks for a specific application can be created using Kaspersky Security Center Web Console only if the management plug-in for that application is installed on Kaspersky Security Center Web Console Server.

Tasks can be performed on the Administration Server and on devices.

The tasks that are performed on the Administration Server include the following:

- Automatic distribution of reports
- Downloading of updates to the repository
- Backup of Administration Server data
- Maintenance of the database

The following types of tasks are performed on devices:

- *Local tasks*—Tasks that are performed on a specific device

  Local tasks can be modified either by the administrator, using Kaspersky Security Center Web Console, or by the user of a remote device (for example, through the security application interface). If a local task has been modified simultaneously by the administrator and the user of a managed device, the changes made by the administrator will take effect because they have a higher priority.

- *Group tasks*—Tasks that are performed on all devices of a specific group

  Unless otherwise specified in the task properties, a group task also affects all subgroups of the selected group. A group task also affects (optionally) devices that have been connected to secondary and virtual Administration Servers deployed in the group or any of its subgroups.

- *Global tasks*—Tasks that are performed on a set of devices, regardless of whether they are included in any group

For each application, you can create any number of group tasks, global tasks, or local tasks.

You can make changes to the settings of tasks, view the progress of tasks, and copy, export, import, and delete tasks.

A task is started on a device only if the application for which the task was created is running.

Execution results of tasks are saved in the operating system event log on each device, in the operating system event log on the Administration Server, and in the Administration Server database.

Do not include private data in task settings. For example, avoid specifying the domain administrator password.

# About task scope

The *scope of a task* is the set of devices on which the task is performed. The types of scope are as follows:

- For a *local task*, the scope is the device itself.
- For an *Administration Server task*, the scope is the Administration Server.
- For a *group task*, the scope is the list of devices included in the group.

When creating a *global task*, you can use the following methods to specify its scope:

- Specifying certain devices manually.

  You can use an IP address (or IP range) or DNS name as the device address. You can also select networked devices detected by Administration Server.

- Importing a list of devices from a .txt file with the device addresses to be added (each address must be placed on an individual line).

  If you import a list of devices from a file or create a list manually, and if devices are identified by their names, the list can only contain devices for which information has already been entered into the Administration Server database. Moreover, the information must have been entered when those devices were connected or during device discovery.

- Specifying a device selection.

  Over time, the scope of a task changes as the set of devices included in the selection change. A selection of devices can be made on the basis of device attributes, including software installed on a device, and on the basis of tags assigned to devices. Device selection is the most flexible way to specify the scope of a task.

  Tasks for device selections are always run on a schedule by the Administration Server. These tasks cannot be run on devices that lack connection to the Administration Server. Tasks whose scope is specified by using other methods are run directly on devices and therefore do not depend on the device connection to the Administration Server.

  Tasks for device selections are not run on the local time of a device; instead, they are run on the local time of the Administration Server. Tasks whose scope is specified by using other methods are run on the local time of a device.

# Creating a task

*To create a task:*

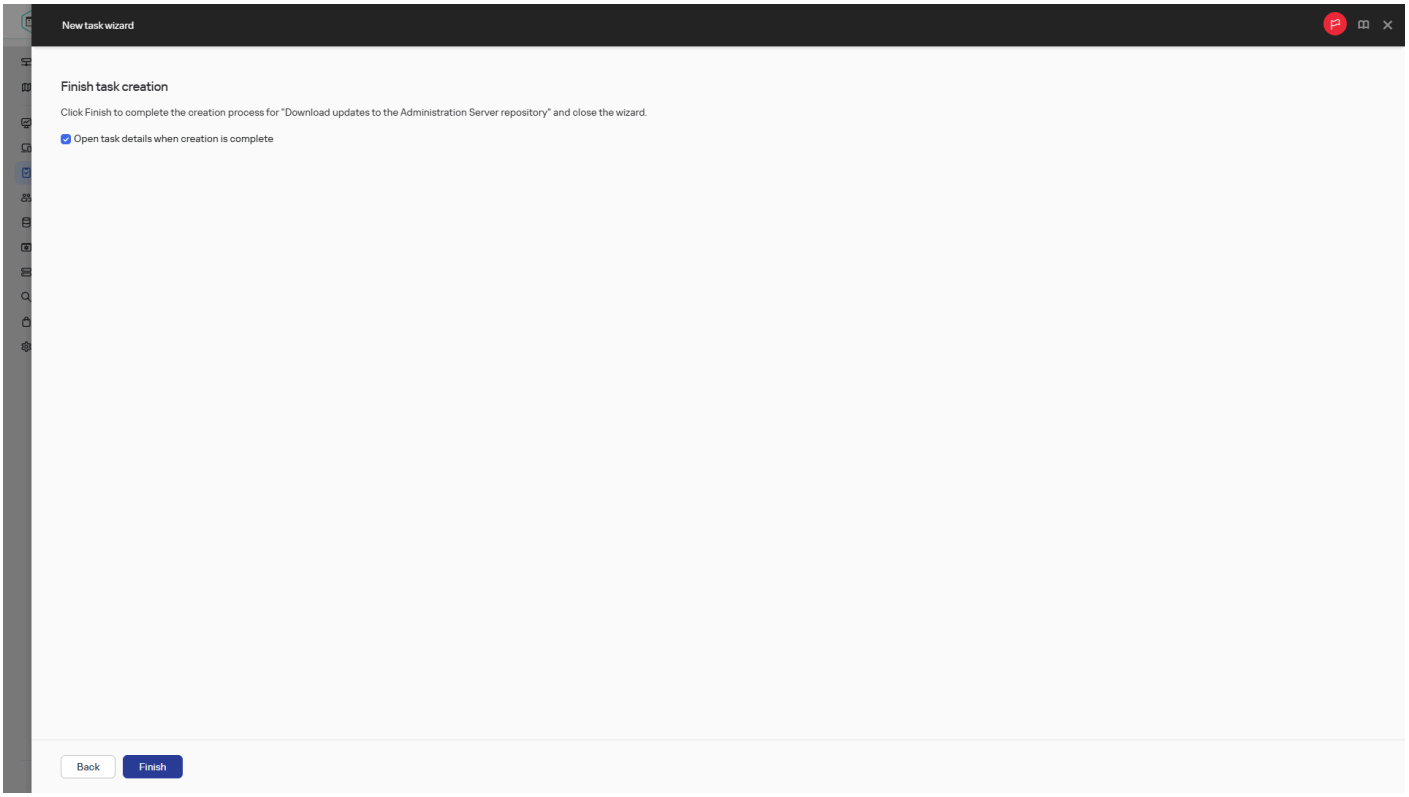
1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts. Follow its instructions.

3. If you want to modify the default task settings, enable the **Open task details when creation is complete** option on the **Finish task creation** page. If you do not enable this option, the task is created with the default settings. You can change the default settings later, at any time.

4. Click the **Finish** button.

The task is created and displayed in the list of tasks.




Finishing task creation

*To create a new task assigned to the selected devices:*

1. In the main menu, go to **Asset management** → **Managed devices**.

   The list of managed devices is displayed.

2. In the list of managed devices, select check boxes next to the devices to run the task for them. You can use the search and filter functions to find the devices you're looking for.

3. Click the **Run task** button, and then select **Add a new task**.

   The New task wizard starts.

   On the first step of the wizard, you can remove the devices selected to include in the task scope. Follow the wizard instructions.

4. Click the **Finish** button.

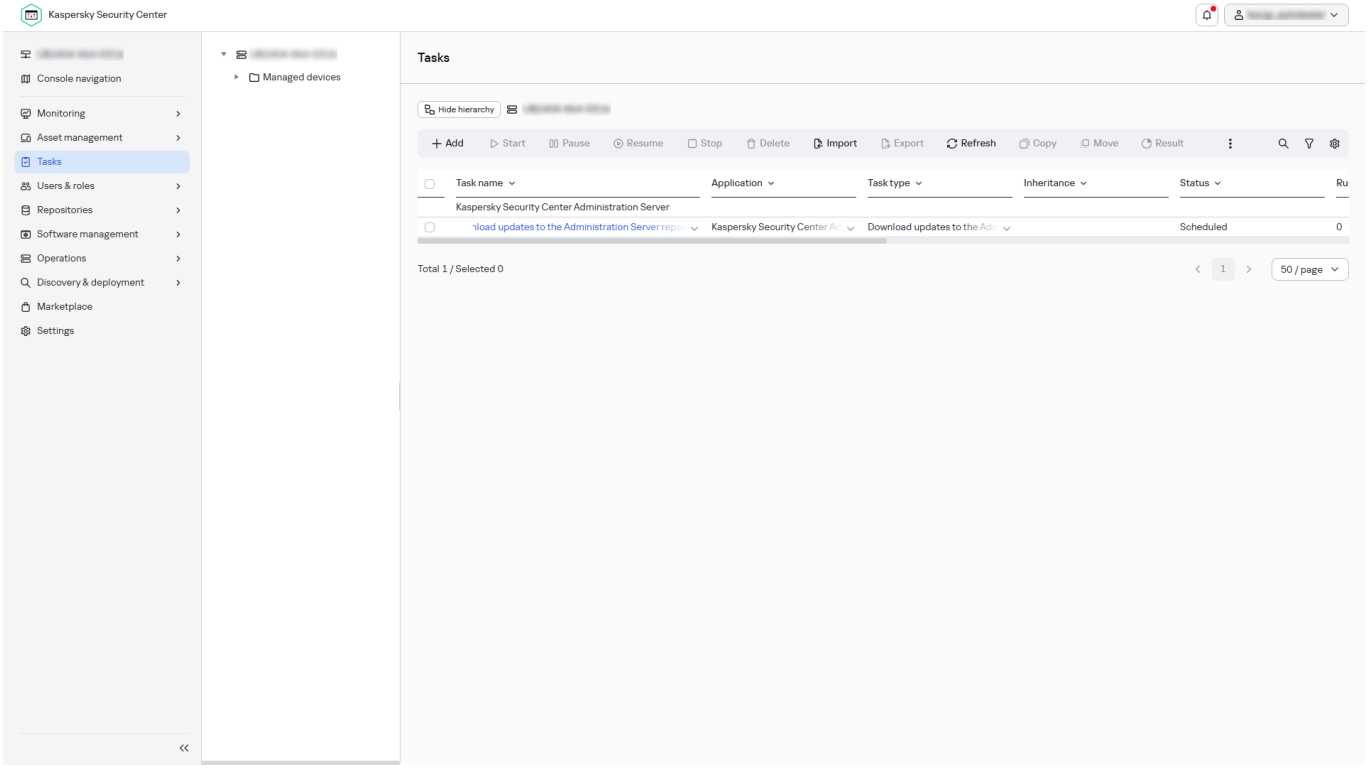
The task is created for the selected devices.

# Starting a task manually

The application starts tasks according to the schedule settings specified in the properties of each task. You can start a task manually at any time from the task list. Alternatively, you can select devices in the **Managed devices** list, and then start an existing task for them.

*To start a task manually:*

1. In the main menu, go to **Tasks**.
2. In the task list, select the check box next to the task that you want to start.
3. Click the **Start** button.




Starting a task from the task list

The task starts. You can check the task status in the **Status** column or by clicking the **Result** button.

# Starting a task for selected devices

You can select one or more client devices in the list of devices, and then launch a previously created task for them. This allows you to run tasks created earlier for a specific set of devices.

This changes the devices to which the task was assigned to the list of devices that you select when you run the task.
The old task scope is deleted and replaced with the selected scope.

*To start a task for selected devices:*

1. In the main menu, go to **Asset management** → **Managed devices**. The list of managed devices is displayed.
2. In the list of managed devices, select check boxes for devices that you want to run the task for. You can use the search and filter functions to find the devices you're looking for.
3. Click the **Run task** button, and then select **Use existing task**.

   The list of existing tasks is displayed.
4. The selected devices are displayed above the task list. If necessary, you can remove a device from this list. You can delete all but one device.
5. Select the desired task in the list. You can use the search box above the list to search for the desired task by name. Only one task can be selected.
6. Save changes by clicking one of the buttons:

   - **Run and close**

     The task is run for the selected devices.

   - **Run and open task**

     The task is run for the selected devices and the task properties window is displayed, in which you can quickly review the task results.

The scheduled start settings in the task are not changed.

# Viewing the task list

You can view the list of tasks that are created in Kaspersky Security Center Linux.

*To view the list of tasks,*

In the main menu, go to **Tasks**.

The list of tasks is displayed. The tasks are grouped by the names of applications to which they are related. For example, the *Install application remotely* task is related to the Administration Server, and the *Update* task refers to Kaspersky Endpoint Security.

*To view properties of a task,*

Click the name of the task.

The task properties window is displayed with several named tabs. For example, the **Task type** is displayed on the **General** tab, and the task schedule—on the **Schedule** tab.

# General task settings

This section contains the settings that you can view and configure for most of your tasks. The list of settings available depends on the task you are configuring.

## Settings specified during task creation

You can specify the following settings when creating a task. Some of these settings can also be modified in the properties of the created task.

- Operating system restart settings:

  **Do not restart the device**

  Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

  **Restart the device**

  Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

  **Force closure of applications in blocked sessions**

  Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

  If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

  If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

  By default, this option is disabled.

- Task scheduling settings:

  > The types of schedule may vary depending on the task.

  > Some types of schedule may be unavailable for other Kaspersky applications.

  - **Start task setting:**

    **Every N hours**

    The task runs regularly, with the specified interval in hours, starting from the specified date and time.

    By default, the task runs every 6 hours, starting from the current system date and time.

    **Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

**Every N minutes**

The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

By default, the task runs every 30 minutes, starting from the current system time.

**By days of week**

The task runs regularly, on the specified days of the week, at the specified time.

By default, the task runs every Friday at 6:00:00 PM.

**Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

**Manually**

The task does not run automatically. You can only start it manually.

By default, this option is selected.

**Once**

The task runs once, on the specified date and time (by default, on the day when the task was created).

**Immediately**

The task runs immediately after its settings are saved.

**Monthly on selected weekday**

The task runs regularly, on the specified days of each month, at the specified time.

By default, the start time is 18:00, and no days of the month are selected.

> Note that you select neither a specific date in the month, nor the number of the week (first, second week of the month) but the sequence number of the weekday within a month. For example, if you set the cursor in the **Tu** cell of the **First** row, it means the task will run every first Tuesday of each new month.

You can select several days of week.

**When new updates are downloaded to the repository**

The task runs after updates are downloaded to the repository. For example, you may want to use this schedule for the *Update* task.

**On completing another task**

The current task starts after another task completes. This option only works if both tasks are assigned to the same devices. For example, you may want to run the *Manage devices* task with the **Turn on the device** option and, after it completes, run the *Virus scan* task as a triggering task.

You have to select the triggering task from the table and the status with which this task must complete (**Completed successfully** or **Failed**).

If necessary, you can search, sort, and filter the tasks in the table as follows:

- Enter the task name in the search field, to search the task by its name.
- Click the sort icon to sort the tasks by name.

  By default, the tasks are sorted in alphabetical ascending order.
- Click the filter icon, and in the window that opens, filter the tasks by group, and then click the **Apply** button.

If you are creating a task for a managed application, and the schedule of the task can be paused, such a task has the following schedule settings:

- **End time**

  The task schedule is stopped at 12:00 a.m. on the specified date. If the task itself is still running when the end time of the schedule arrives, the task is not terminated.

  For example, suppose a task runs at 11:00 p.m. every day. You specify that on January 1, the schedule for this task will be terminated. On December 31, the task runs at 11:00 p.m., and on January 1 at 12:00 a.m., its schedule is paused: the task continues to run until completion, and after 11:00 p.m. on January 1, the schedule is no longer triggers.

  This option is available for all schedule types, except **Manually** and **Once**.
- **Pause task**

  If this setting is enabled, you can specify a time interval during which a task previously started on a schedule must be paused. For example, from 10:00 a.m. to 11:00 a.m.

  This may be necessary during peak device use periods to reduce the impact of the managed application (for example, Kaspersky Endpoint Security) on performance.

  This option is available for all schedule types.

- **Run missed tasks**

  This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

  If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

  If this option is disabled, only scheduled tasks run on client devices. For **Manually**, **Once** and **Immediately** schedule, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

  By default, this option is enabled.

- **Use automatically randomized delay for task starts**

  If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However, when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is enabled.

- **Use automatically randomized delay for task starts within an interval of**

  If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

  If this option is disabled, the task starts on client devices according to the schedule.

  By default, this option is disabled. The default time interval is one minute.

- Devices to which the task will be assigned:

  **Select networked devices detected by Administration Server**

  The task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.

  For example, you may want to use this option in a task of installing Network Agent on unassigned devices.

  **Specify device addresses manually or import addresses from list**

  You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

  You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

  **Assign task to a device selection**

  The task is assigned to devices included in a device selection. You can specify one of the existing selections.

  For example, you may want to use this option to run a task on devices with a specific operating system version.

  **Assign task to an administration group**

  The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

  For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

  If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

- Account settings:

  **Default account**

  The task will be run under the same account as the application that performs this task.

  By default, this option is selected.

  **Specify an account**

  Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

  **Login.**

  Account under which the task is run.

**Password**

Password of the account under which the task will be run.

## Settings specified after task creation

You can specify the following settings only after a task is created.

- Group task settings:

  **Distribute to subgroups**

  This option is only available in the settings of the group tasks.

  When this option is enabled, the task scope includes:

  - The administration group that you selected while creating the task.
  - The administration groups subordinate to the selected administration group at any level down by the group hierarchy.

  When this option is disabled, the task scope includes only the administration group that you selected while creating the task.

  By default, this option is enabled.

  **Distribute to secondary and virtual Administration Servers**

  When this option is enabled, the task that is effective on the primary Administration Server is also applied on the secondary Administration Servers (including virtual ones). If a task of the same type already exists on the secondary Administration Server, both tasks are applied on the secondary Administration Server—the existing one and the one that is inherited from the primary Administration Server.

  This option is only available when the **Distribute to subgroups** option is enabled.

  By default, this option is disabled.

- Advanced scheduling settings:

  **Turn on devices by using the Wake-on-LAN function before starting the task**

  The operating system on the device starts at the specified time before the task is started. The default time period is five minutes.

  Enable this option if you want the task to run on all of the client devices from the task scope, including those devices that are turned off when the task is about to start.

  If you want the device to be automatically turned off after the task is completed, enable the **Shut down the devices after completing the task** option. This option can be found in the same window.

  By default, this option is disabled.

  **Shut down the devices after completing the task**

  For example, you may want to enable this option for an install update task that installs updates to client devices each Friday after business hours, and then turns off these devices for the weekend.

  By default, this option is disabled.

  **Stop the task if it runs longer than**

After the specified time period expires, the task is stopped automatically, whether it is completed or not.

Enable this option if you want to interrupt (or stop) tasks that take too long to execute.

By default, this option is disabled. The default task execution time is 120 minutes.

- Notification settings:
  - **Store task history** block:

    **Store in the Administration Server database for (days)**

    Application events related to execution of the task on all client devices from the task scope are stored on the Administration Server during the specified number of days. When this period elapses, the information is deleted from the Administration Server.

    By default, this option is enabled.

    **Store in the OS event log on device**

    Application events related to execution of the task are stored locally in the Syslog Event Log of each client device.

    By default, this option is disabled.

    **Store in the OS event log on Administration Server**

    Application events related to execution of the task on all client devices from the task scope are stored centrally in the Syslog Event Log of the Administration Server operating system (OS).

    By default, this option is disabled.

    **Save all events**

    If this option is selected, all events related to the task are saved to the event logs.

    **Save events related to task progress**

    If this option is selected, only events related to the task execution are saved to the event logs.

    **Save only task execution results**

    If this option is selected, only events related to the task results are saved to the event logs.

  - **Notify administrator of task execution results**

    You can select the methods by which administrators receive notifications about task execution results: by email, by SMS, and by running an executable file. To configure notification, click the **Settings** link.

    By default, all notification methods are disabled.

  - **Notify of errors only**

    If this option is enabled, administrators are only notified when a task execution completes with an error.

    If this option is disabled, administrators are notified after every task execution completion.

    By default, this option is enabled.

- Security settings.

- Task scope settings.

  Depending on how the task scope is determined, the following settings are present:

  **Devices**

  If the scope of a task is determined by an administration group, you can view this group. No changes are available here. However, you can set **Exclusions from task scope**.

  If the scope of a task is determined by a list of devices, you can modify this list by adding and removing devices.

  **Device selection**

  You can change the device selection to which the task is applied.

  **Exclusions from task scope**

  You can specify groups of devices to which the task is not applied. Groups to be excluded can only be subgroups of the administration group to which the task is applied.

- **Revision history**.

# Exporting a task

Kaspersky Security Center Linux allows you to save a task and its settings to a KLT file. You can use this KLT file to import the saved task both to Kaspersky Security Center Windows and Kaspersky Security Center Linux.

*To export a task:*

1. In the main menu, go to **Tasks**.
2. Select the check box next to the task that you want to export.

   You cannot export multiple tasks at the same time. If you select more than one task, the **Export** button will be disabled. Administration Server tasks are also unavailable for export.
3. Click the **Export** button.
4. In the opened **Save as** window, specify the task file name and path. Click the **Save** button.

   The **Save as** window is displayed only if you use Google Chrome, Microsoft Edge, or Opera. If you use another browser, the task file is automatically saved in the **Downloads** folder.

# Importing a task

Kaspersky Security Center Linux allows you to import a task from a KLT file. The KLT file contains the exported task and its settings.

For correct import of the Kaspersky application task, you have to install the appropriate management plug-in.

*To import a task:*

1. In the main menu, go to **Tasks**.
2. Click the **Import** button.
3. Click the **Browse** button to choose a task file that you want to import.
4. In the opened window, specify the path to the KLT task file, and then click the **Open** button. Note that you can select only one task file.

   The task processing starts.
5. After the task is processed successfully, select the devices to which you want to assign the task. To do this, select one of the following options:

   **Assign task to an administration group**

   The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

   For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

   If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

   **Specify device addresses manually or import addresses from a list**

   You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

   You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

   **Assign task to a device selection**

   The task is assigned to devices included in a device selection. You can specify one of the existing selections.

   For example, you may want to use this option to run a task on devices with a specific operating system version.
6. Specify the task scope.
7. Click the **Complete** button to finish the task import.

The notification with the import results appears. If the task is imported successfully, you can click the **Details** link to view the task properties.

After a successful import, the task is displayed in the task list. The task settings and schedule are also imported. The task will be started according to its schedule.

> If the newly imported task has an identical name to an existing task, the name of the imported task is expanded with the **(<next sequence number>)** index, for example: **(1)**, **(2)**.

# Starting the Change tasks password wizard

For a non-local task, you can specify an account under which the task must be run. You can specify the account during task creation or in the properties of an existing task. If the specified account is used in accordance with security instructions of the organization, these instructions might require changing the account password from time to time. When the account password expires and you set a new one, the tasks will not start until you specify the new valid password in the task properties.

The Change tasks password wizard enables you to automatically replace the old password with the new one in all tasks in which the account is specified. Alternatively, you can change this password manually in the properties of each task.

*To start the Change tasks password wizard:*

1. In the main menu, go to **Tasks**.
2. Click **Manage credentials of accounts for starting tasks**.

Follow the steps of the wizard.

## Step 1. Specifying credentials

Specify new credentials that are currently valid in your system. When you switch to the next step of the wizard, Kaspersky Security Center Linux checks if the specified account name matches the account name in the properties of each non-local task. If the account names match, the password in the task properties will be automatically replaced with the new one.

To specify the new account, select an option:

**Use current account**

The wizard uses the name of the account under which you are currently signed in to Kaspersky Security Center Web Console. Then manually specify the account password in the **Current password to use in tasks** field.

**Specify a different account**

Specify the name of the account under which the tasks must be started. Then specify the account password in the **Current password to use in tasks** field.

If you fill in the **Previous password (optional; if you want to replace it with the current one)** field, Kaspersky Security Center Linux replaces the password only for those tasks in which both the account name and the old password are found. The replacement is performed automatically. In all other cases you have to choose an action to take in the next step of the wizard.

## Step 2. Selecting an action to take

If you did not specify the previous password in the first step of the wizard or if the specified old password has not matched the passwords in the task properties, you must choose an action to take for the tasks found.

*To choose an action for a task:*

1. Select the check box next to the task for which you want to choose an action.
2. Do one of the following:
   - To remove the password in the task properties, click **Delete credentials**.
     The task is switched to run under the default account.
   - To replace the password with a new one, click **Enforce the password change even if the old password is wrong or not provided**.
   - To cancel the password change, click **No action is selected**.

The chosen actions are applied after you move to the next step of the wizard.

### Step 3. Viewing the results

On the last step of the wizard, view the results for each of the found tasks. To complete the wizard, click the **Finish** button.

## Viewing task run results stored on the Administration Server

Kaspersky Security Center Linux allows you to view the results for group tasks, tasks for specific devices, and Administration Server tasks.

*To view the task results:*

In the task properties window, go to the **Results** tab.

*To view task results for a secondary Administration Server:*

1. In the task properties window, select the **General** section.
2. Click the **Results** link to open the **Task results** window.
3. Click **Statistics from secondary Servers**.
4. Select the secondary Server for which you want to display the **Task results** window.

# Application tags

This section describes application tags, and provides instructions for creating and modifying them as well as for tagging third-party applications.

# Application tags

Kaspersky Security Center Linux enables you to tag the applications from applications registry. A tag is the label of an application that can be used for grouping or finding applications. A tag assigned to applications can serve as a condition in device selections.

For example, you can create the `[Browsers]` tag and assign it to all browsers such as Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

# Creating an application tag

*To create an application tag:*

1. In the main menu, go to **Software management** → **Third-party applications** → **Application tags**.
2. Click **Add**.

   A new tag window opens.
3. Enter the tag name.
4. Click **OK** to save the changes.

The new tag appears in the list of application tags.

# Renaming an application tag

*To rename an application tag:*

1. In the main menu, go to **Software management** → **Third-party applications** → **Application tags**.
2. Select the check box next to the tag that you want to rename, and then click **Edit**.

   A tag properties window opens.
3. Change the tag name.
4. Click **OK** to save the changes.

The updated tag appears in the list of application tags.

# Assigning tags to an application

*To assign one or several tags to an application:*

1. In the main menu, go to **Software management** → **Third-party applications** → **Applications registry**.
2. Click the name of the application to which you want to assign tags.
3. Select the **Tags** tab.

   The tab displays all application tags that exist on the Administration Server. For tags assigned to the selected application, the check box in the **Tag assigned** column is selected.
4. For tags that you want to assign, select check boxes in the **Tag assigned** column.
5. Click **Save** to save changes.

The tags are assigned to the application.

# Removing assigned tags from an application

*To remove one or several tags from an application:*

1. In the main menu, go to **Software management** → **Third-party applications** → **Applications registry**.
2. Click the name of the application from which you want to remove tags.
3. Select the **Tags** tab.

   The tab displays all application tags that exist on the Administration Server. For tags assigned to the selected application, the check box in the **Tag assigned** column is selected.
4. For tags that you want to remove, clear check boxes in the **Tag assigned** column.
5. Click **Save** to save changes.

The tags are removed from the application.

The removed application tags are not deleted. If you want, you can delete them manually.

# Deleting an application tag

*To delete an application tag:*

1. In the main menu, go to **Software management** → **Third-party applications** → **Application tags**.
2. In the list, select the application tag that you want to delete.
3. Next, click the **Delete** button.
4. In the window that opens, click **OK**.

The application tag is deleted. The deleted tag is automatically removed from all of the applications to which it was assigned.

# Using the klscflag utility to open port 13291

You can automate the Kaspersky Security Center Linux operation using the klakaut utility. The klakaut utility and a Help system for it are located in the Kaspersky Security Center Linux installation folder. If you want to use the klakaut utility, open the 13291 port by using the klscflag utility.

The klscflag utility changes the value of the KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN parameter.

*To open port 13291:*

1. Execute the following command in the command line:
   ```
   /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
   KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
   \"SS_SETTINGS\";"
   ```
2. Restart the Kaspersky Security Center Administration Server service by executing the following command:
   ```
   sudo systemctl restart kladminserver_srv
   ```

Port 13291 is open.

*To check if port 13291 has been successfully open:*

Execute the following command in the command line:

```
/opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

This command returns the following result:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

The `true` value means that the port is open. Otherwise, the `false` value is displayed.

# Registering Kaspersky Industrial CyberSecurity for Networks application in Kaspersky Security Center Web Console

To start working with the Kaspersky Industrial CyberSecurity for Networks application via Kaspersky Security Center Web Console, you must first register it in Kaspersky Security Center Web Console.

*To register the Kaspersky Industrial CyberSecurity for Networks application:*

1. Make sure that the following is done:

   - You have downloaded and installed the Kaspersky Industrial CyberSecurity for Networks web plug-in.

     You can do it later while waiting for the Kaspersky Industrial CyberSecurity for Networks Server to synchronize with the Administration Server. After the plug-in is downloaded and installed, the **KICS for Networks** section is displayed in the Kaspersky Security Center Web Console main menu.

   - In the Kaspersky Industrial CyberSecurity for Networks web interface, interaction with Kaspersky Security Center Linux is configured and enabled. For details, refer to the Kaspersky Industrial CyberSecurity for Networks Help.

2. Move the device where Kaspersky Industrial CyberSecurity for Networks Server is installed from the Unassigned devices group to the Managed devices group:

   a. In the main menu, go to **Asset management** → **Unassigned devices**.

   b. Select the check box next to the device where the Kaspersky Industrial CyberSecurity for Networks Server is installed.

   c. Click the **Move to group** button.

   d. In the hierarchy of administration groups, select the check box next to the **Managed devices** group.

   e. Click the **Move** button.

3. Open the properties window of the device where the Kaspersky Industrial CyberSecurity for Networks Server is installed.

4. On the device properties page, in the **General** section, select the **Do not disconnect from the Administration Server** option, and then click the **Save** button.

5. On the device properties page, select the **Applications** section.

6. In the **Applications** section, select Kaspersky Security Center Network Agent.

7. If the current status of the application is *Stopped*, wait until it changes to *Running*.

   This may take up to 15 minutes. If you have not yet installed the Kaspersky Industrial CyberSecurity for Networks web plug-in, you can do it now.

8. If you want to view the statistics of Kaspersky Industrial CyberSecurity for Networks, you may add widgets on the dashboard. To add the widgets, do the following:

   a. In the main menu, go to **Monitoring** → **Dashboard**.

   b. On the dashboard, click the **Add or restore web widget** button.

   c. In the widget menu that opens, select **Other**.

   d. Select the widgets that you want to add:

      - KICS for Networks deployment map
      - Information about KICS for Networks Servers
      - Up-to-date events of KICS for Networks
      - Devices with issues in KICS for Networks
      - Critical events in KICS for Networks
      - Statuses in KICS for Networks

9. To proceed to the Kaspersky Industrial CyberSecurity for Networks web interface, do the following:

   a. In the main menu, go to **KICS for Networks** → **Search**.

   b. Click the **Find events or devices** button.

   c. In the **Query parameters** window that opens, click the **Server** field.

   d. Select the Kaspersky Industrial CyberSecurity for Networks Server from the drop-down list of servers that are integrated with Kaspersky Security Center Linux, and then click the **Find** button.

   e. Click the **Go to Server** link next to the name of the Kaspersky Industrial CyberSecurity for Networks Server.

   The Kaspersky Industrial CyberSecurity for Networks sign-in page is displayed.

   > To log in to the Kaspersky Industrial CyberSecurity for Networks web interface, you need to provide the application user account credentials.

# Managing users and user roles

This section describes users and user roles, and provides instructions for creating and modifying them, for assigning roles and groups to users, and for associating policy profiles with roles.

## About user accounts

Kaspersky Security Center Linux allows you to manage user accounts and security groups. The application supports three types of accounts:

- Accounts of organization employees. Administration Server retrieves data of the accounts of those domain users when polling the organization's domain controller.
- Accounts of local users. Local accounts on managed devices, as well as the local accounts on the device on which Administration Server is installed.
- Accounts of internal users of Kaspersky Security Center Linux. You can create accounts of internal users. These accounts are used only within Kaspersky Security Center Linux.

Local user accounts and the local kladmins group in the Linux operating system cannot be used for access to the Kaspersky Security Center Web Console in Kaspersky Security Center Linux. The kladmins group can only contain accounts that are used to start Kaspersky Security Center Linux services. Employees of the organization will be able to use their user accounts to log in after configuring domain authentication.

*To view tables of user accounts and security groups:*

1. In the main menu, go to **Users & roles** → **Users & groups**.
2. Select the **Users** or the **Groups** tab.

The table of users or security groups opens. If you want to view the table with only internal users or groups or with only local users or groups, set the **Account type** filter criteria to **Internal** or **Local** respectively.

If the table of users contains more than 50,000 users, only the first 50,000 users are displayed, and the remaining users are not shown.

# About user roles

A *user role* (also referred to as a *role*) is an object containing a set of rights and privileges. A role can be associated with settings of Kaspersky applications installed on a user device. You can assign a role to a set of users or to a set of security groups at any level in the hierarchy of administration groups, Administration Servers, or at the level of specific objects.

If you manage devices through a hierarchy of Administration Servers that includes virtual Administration Servers, note that you can create, modify, or delete user roles only from a physical Administration Server. Then, you can propagate the user roles to secondary Administration Servers, including virtual ones.

You can associate user roles with policy profiles. If a user is assigned a role, this user gets security settings necessary to perform job functions.

A user role can be associated with users of devices in a specific administration group.

## User role scope

A *user role scope* is a combination of users and administration groups. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.

## Advantage of using roles

An advantage of using roles is that you do not have to specify security settings for each of the managed devices or for each of the users separately. The number of users and devices in a company may be quite large, but the number of different job descriptions that require different security settings is considerably smaller.

## Differences from using policy profiles

Policy profiles are properties of a policy that is created for each Kaspersky application separately. A role is associated with many policy profiles created for different applications. Therefore, a role is a method of uniting settings for a certain user type in one place.

# Configuring access rights to application features. Role-based access control

Kaspersky Security Center Linux provides facilities for role-based access to the features of Kaspersky Security Center Linux and managed Kaspersky applications.

You can configure access rights to application features for Kaspersky Security Center Linux users in one of the following ways:

- By configuring the rights for each user or group of users individually.
- By creating standard user roles with a predefined set of rights and assigning those roles to users depending on their scope of duties.

Application of user roles is intended to simplify and shorten routine procedures of configuring users' access rights to application features. Access rights within a role are configured in accordance with the standard tasks and the users' scope of duties.

User roles can be assigned names that correspond to their respective purposes. You can create an unlimited number of roles in the application.

You can use the predefined user roles with already configured set of rights, or create new roles and configure the required rights yourself.

## Access rights to application features

The table below shows the Kaspersky Security Center Linux features with the access rights to manage the associated tasks, reports, settings, and perform the associated user actions.

To perform the user actions listed in the table, a user has to have the right specified next to the action.

**Read**, **Write**, and **Execute** rights are applicable to any task, report, or setting. In addition to these rights, a user has to have the **Perform operations on device selections** right to manage tasks, reports, or settings on device selections.

> All tasks, reports, settings, and installation packages that are missing in the table belong to the **General features: Basic functionality** functional area.

| Functional area | Right | User action: right required to perform the action | Task | Report | Other |
|---|---|---|---|---|---|
| **General features**: **Management of administration groups** | **Write** | • Add device to an administration group: **Write**<br>• Delete device from an administration group: **Write**<br>• Add an administration group to another administration group: **Write**<br>• Delete an administration group from another administration group: **Write** | None | None | None |

| Functional area | Right | User action: right required to perform the action | Task | Report | Other |
|---|---|---|---|---|---|
| **General features**: **Access objects regardless of their ACLs** | **Read** | Get read access to all objects: **Read** | None | None | The **General features: Access objects regardless of their ACLs** functional area is intended for audit purposes. A **Read** permission in this functional area grants full **Read** access to all objects. We recommend granting these rights carefully and to a limited set of users who need them to perform their official duties.<br>Access is granted regardless of other rights, even if they prohibit read access to specific objects. |
| **General features**: **Basic functionality** | • **Read**<br>• **Write**<br>• **Execute**<br>• **Perform operations on device selections** | • Device moving rules (create, modify, or delete) for the virtual Server: **Write**, **Perform operations on device selections**<br>• Get Mobile (LWNGT) protocol custom certificate: **Read**<br>• Set Mobile (LWNGT) protocol custom certificate: **Write**<br>• Get NLA-defined network list: **Read**<br>• Add, modify, or delete NLA-defined network list: **Write**<br>• View Access Control List of groups: **Read**<br>• View the operating system log: **Read**<br>• View the recovery key to restore access to a hard drive encrypted by BitLocker: **Execute** | • "Download updates to the Administration Server repository"<br>• "Deliver reports"<br>• "Distribute installation package"<br>• "Install application on secondary Administration Servers remotely" | • "Report on protection status"<br>• "Report on threats"<br>• "Report on most heavily infected devices"<br>• "Report on status of anti-virus databases"<br>• "Report on errors"<br>• "Report on network attacks"<br>• "Summary report on mail system protection applications installed"<br>• "Summary report on workstation protection and Windows Server protection applications installed"<br>• "Summary report on perimeter defense applications installed"<br>• "Summary report on types of applications installed"<br>• "Report on users of infected devices"<br>• "Report on security issues"<br>• "Report on events"<br>• "Report on activity of distribution points"<br>• "Report on secondary Administration Servers" | None |

| Functional area | Right | User action: right required to perform the action | Task | Report | Other |
|---|---|---|---|---|---|
| | | | | • "Report on Device Control events"<br>• "Report on vulnerabilities"<br>• "Report on prohibited applications"<br>• "Report on Web Control"<br>• "Report on encryption status of managed devices"<br>• "Report on encryption status of mass storage devices"<br>• "Report on rights to access encrypted drives"<br>• "Report on file encryption errors"<br>• "Report on blockage of access to encrypted files"<br>• "Report on effective user permissions"<br>• "Report on rights" | |
| **General features**: **Deleted objects** | • **Read**<br>• **Write** | • View deleted objects in the Recycle Bin: **Read**<br>• Delete objects from the Recycle Bin: **Write** | None | None | None |
| **General features**: **Event processing** | • **Delete events**<br>• **Edit event notification settings**<br>• **Edit event logging settings**<br>• **Write** | • Change events registration settings: **Edit event logging settings**<br>• Change events notification settings: **Edit event notification settings**<br>• Delete events: **Delete events** | None | None | Settings:<br>• The maximum number of events stored in the database<br>• Period for storing events from the deleted devices |
| **General features**: **Operations on Administration Server** | • **Read**<br>• **Write**<br>• **Execute**<br>• **Modify object ACLs**<br>• **Perform operations on device selections** | • Specify ports of Administration Server for the network agent connection: **Write**<br>• Specify ports of Activation Proxy launched on the Administration Server: **Write**<br>• Specify ports of Activation Proxy for Mobile launched on the Administration Server: **Write**<br>• Specify ports of the Web Server for distribution of standalone packages: **Write** | • "Backup of Administration Server data"<br>• "Databases maintenance" | None | None |

| Functional area | Right | User action: right required to perform the action | Task | Report | Other |
|---|---|---|---|---|---|
| | | • Specify ports of the Web Server for distribution of MDM profiles: **Write**<br>• Specify SSL-ports of the Administration Server for connection via Web Console: **Write**<br>• Specify ports of the Administration Server for mobile connection: **Write**<br>• Specify the maximum number of events stored in the Administration Server database: **Write**<br>• Specify the maximum number of events that can be sent by the Administration Server: **Write**<br>• Specify time period during which events can be sent by the Administration Server: **Write** | | | |
| **General features**: **Kaspersky software deployment** | • **Manage Kaspersky patches**<br>• **Read**<br>• **Write**<br>• **Execute**<br>• **Perform operations on device selections** | Approve or decline installation of the patch: **Manage Kaspersky patches** | None | • "Report on license key usage by virtual Administration Server"<br>• "Report on Kaspersky software versions"<br>• "Report on incompatible applications"<br>• "Report on versions of Kaspersky software module updates"<br>• "Report on protection deployment" | Installation package:<br>"Kaspersky" |
| **General features**: **Key management** | • **Export key file**<br>• **Write** | • Export key file: **Export key file**<br>• Modify Administration Server license key settings: **Write** | None | None | None |
| **General features**: **Enforced report management** | • **Read**<br>• **Write** | • Create reports regardless of their ACLs: **Write**<br>• Execute reports regardless of their ACLs: **Read** | None | None | None |
| **General features**: **Hierarchy of Administration Servers** | **Configure hierarchy of Administration Servers** | • Register, update, or delete secondary Administration Servers: **Configure hierarchy of** | None | None | None |

| Functional area | Right | User action: right required to perform the action | Task | Report | Other |
|---|---|---|---|---|---|
| | | **Administration Servers** | | | |
| **General features**: **User permissions** | **Modify object ACLs** | • Change Security properties of any object: **Modify object ACLs**<br>• Manage user roles: **Modify object ACLs**<br>• Manage internal users: **Modify object ACLs**<br>• Manage security groups: **Modiobject ACLs**<br>• Manage aliases: **Modify object ACLs** | None | None | None |
| **General features**: **Virtual Administration Servers** | • **Manage virtual Administration Servers**<br>• **Read**<br>• **Write**<br>• **Execute**<br>• **Perform operations on device selections** | • Get list of virtual Administration Servers: **Read**<br>• Get information on the virtual Administration Server: **Read**<br>• Create, update, or delete a virtual Administration Server: **Manage virtual Administration Servers**<br>• Move a virtual Administration Server to another group: **Manage virtual Administration Servers**<br>• Set administration virtual Server permissions: **Manage virtual Administration Servers** | None | None | None |

| Functional area | Right | User action: right required to perform the action | Task | Report | Other |
|---|---|---|---|---|---|
| **General features**: Encryption Key Management | **Write** | Import the encryption keys: **Write** | None | None | None |
| **Mobile device management**: General | • **Connect new devices**<br>• **Send only information commands to mobile devices**<br>• **Send commands to mobile devices**<br>• **Manage certificates**<br>• **Read**<br>• **Write** | • Get Key Management Service restore data: **Read**<br>• Delete user certificates: **Manage certificates**<br>• Get user certificate public part: **Read**<br>• Check if Public Key Infrastructure is enabled: **Read**<br>• Check Public Key Infrastructure account: **Read**<br>• Get Public Key Infrastructure templates: **Read**<br>• Get Public Key Infrastructure templates by Extended Key Usage certificate: **Read**<br>• Check if Public Key Infrastructure certificate is revoked: **Read**<br>• Update user certificate issuance settings: **Manage certificates**<br>• Get user certificate issuance settings: **Read**<br>• Get packages by application name and version: **Read**<br>• Set or cancel user certificate: **Manage certificates**<br>• Renew user certificate: **Manage certificates**<br>• Set user certificate tag: **Manage certificates**<br>• Run generation of MDM installation package; cancel generation of MDM installation package: **Connect new devices** | None | None | None |
| **System management**: Connectivity | • **Start RDP sessions**<br>• **Connect to existing RDP sessions**<br>• **Initiate tunneling** | • Create desktop sharing session: **The right to create desktop sharing session**<br>• Create RDP session: **Connect** | None | "Report on device users" | None |

| Functional area | Right | User action: right required to perform the action | Task | Report | Other |
|---|---|---|---|---|---|
| | • **Save files from devices to the administrator's workstation**<br>• **Read**<br>• **Write**<br>• **Execute**<br>• **Perform operations on device selections** | **to existing RDP sessions**<br>• Create tunnel: **Initiate tunneling**<br>• Save content network list: **Save files from devices to the administrator's workstation** | | | |
| **System management: Vulnerability and patch management** | • **Read**<br>• **Write**<br>• **Execute**<br>• **Perform operations on device selections** | • View third-party patch properties: **Read**<br>• Change third-party patch properties: **Write** | • "Fix vulnerabilities"<br>• "Install required updates and fix vulnerabilities" | "Report on software updates" | None |
| **System management: Execute scripts remotely** | • **Read**<br>• **Write**<br>• **Execute**<br>• **Perform operations on device selections** | User can view the task properties: **Read**<br>User can create, delete or modify an installation package: **Write**<br>User can run a task: **Write**. On client Linux devices scripts are executed with root privileges.<br>User can run a task or schedule it to run: **Execute**<br>User can run a task on a selection of devices: **Perform operations on device selections** | "Execute scripts remotely" | None | None |

# Predefined user roles

User roles assigned to Kaspersky Security Center Linux users provide them with sets of access rights to application features.

Users created on a virtual Server cannot be assigned a role on the Administration Server.

You can use the predefined user roles with already configured set of rights, or create new roles. When creating a new role, you have to set the role scope and assign access rights to the Kaspersky Security Center Linux features yourself. Some of the predefined user roles available in Kaspersky Security Center Linux can be associated with specific job positions, for example, **Auditor**, **Security Officer**, **Supervisor**. Access rights of these roles are pre-configured in accordance with the standard tasks and scope of duties of the associated positions. The table below shows how roles can be associated with specific job positions.

Examples of roles for specific job positions

| Role | Comment |
|---|---|
| Auditor | Permits all viewing operations and executing any created tasks on selections of devices connected to the Administration Server via Network Agent with local administrator rights (root for Linux).<br><br>We recommend assigning this role carefully and to a limited set of users who need them to perform their official duties. |
| Supervisor | Permits all viewing operations; does not permit other operations. You can assign this role to a security officer and other managers in charge of the IT security in your organization. |
| Security Officer | Permits all viewing operations, permits reports management; grants limited permissions in the **System management**: **Connectivity** area. You can assign this role to an officer in charge of the IT security in your organization. |

The table below shows the access rights assigned to each predefined user role.

Access rights of predefined user roles

| Role | Description |
|---|---|
| Administration Server Administrator | Permits all operations in the following functional areas:<br>• **General features**:<br>  • **Basic functionality**<br>  • **Encryption key management**<br>  • **Event processing**<br>  • **Hierarchy of Administration Servers**<br>  • **Virtual Administration Servers**<br>• **System management**:<br>  • **Connectivity**<br>  • **Hardware inventory**<br>  • **Software inventory** |
| Administration Server Operator | Grants the **Read** and **Execute** (where applicable) rights in all of the following functional areas:<br>• **General features**:<br>  • **Basic functionality**<br>  • **Encryption key management**<br>  • **Virtual Administration Servers**<br>• **System management**:<br>  • **Connectivity**<br>  • **Hardware inventory**<br>  • **Software inventory** |
| Auditor | Permits all operations in the following functional areas, in **General features**:<br>• **Access objects regardless of their ACLs**<br>• **Deleted objects**<br>• **Enforced report management**<br>You can assign this role to a person who performs the audit of your organization. |

| Role | Description |
| --- | --- |
| Installation Administrator | Permits all operations in the following functional areas:<br>• **General features:**<br>  • **Basic functionality**<br>  • **Kaspersky application deployment**<br>  • **License key management**<br>• **System Management:**<br>  • **Deploy operating system**<br>  • **Vulnerability and patch management**<br>  • **Remote installation**<br>  • **Software inventory**<br>Grants **Read** and **Execute** rights in the **General features: Virtual Administration Servers** functional area. |
| Installation Operator | Grants the **Read** and **Execute** (where applicable) rights in all of the following functional areas:<br>• **General features:**<br>  • **Basic functionality**<br>  • **Kaspersky software deployment** (also grants the **Manage Kaspersky Lab patches** right in this area)<br>  • **Virtual Administration Servers**<br>• **System Management:**<br>  • **Deploy operating system**<br>  • **Vulnerability and patch management**<br>  • **Remote installation**<br>  • **Software inventory** |
| Kaspersky Endpoint Security Administrator | Permits all operations in the following functional areas:<br>• **General features: Basic functionality**<br>• **General features: Encryption key management**<br>• **Kaspersky Endpoint Security** area, including all features |
| Kaspersky Endpoint Security Operator | Grants the **Read** and **Execute** (where applicable) rights in all of the following functional areas:<br>• **General features: Basic functionality**<br>• **General features: Encryption key management**<br>• **Kaspersky Endpoint Security** area, including all features |
| General administrator | Permits all operations in functional areas, *except* for the following areas, in **General features**:<br>• **Access objects regardless of their ACLs**<br>• **Enforced report management** |
| Main Operator | Grants the **Read** and **Execute** (where applicable) rights in all of the following functional areas:<br>• **General features**:<br>  • **Basic functionality**<br>  • **Deleted objects**<br>  • **Encryption key management**<br>  • **Operations with Administration Server**<br>  • **Device tags**<br>  • **Kaspersky application deployment**<br>  • **Application integration**<br>  • **Virtual Administration Servers**<br>• **Mobile Device Management** area, including all features<br>• **System management** area, including all features<br>• **Kaspersky Endpoint Security** area, including all features |

| Role | Description |
|---|---|
| Mobile Device Management Administrator | Permits all operations in the following functional areas:<br>• **General features: Basic functionality**<br>• **Mobile Device Management** area, including all features<br>Grants the **Export key file** right in the **General features: License key management**.<br>Grants the **Read** right in the **System management: Vulnerability and patch management**. |
| Mobile Device Management Operator | Grants the **Read** and **Execute** rights in the **General features: Basic functionality**.<br>Grants the **Read** and **Send only information commands to mobile devices** rights, in **Mobile Device Management**:<br>• **Common**<br>• **Self Service Portal** |
| Security Officer | Permits all operations in the following functional areas, in **General features**:<br>• **Access objects regardless of their ACLs**<br>• **Enforced report management**<br>Grants the following rights in the **System management: Connectivity** functional area: **Read**, **Write**, **Execute**, **Save files from devices to the administrator's workstation**, and **Perform operations on device selections**.<br>You can assign this role to an officer in charge of the IT security in your organization. |
| Self Service Portal User | Permits all operations in the **Mobile Device Management: Self Service Portal** functional area. |
| Supervisor | Grants the **Read** right in the **General features**: **Access objects regardless of their ACLs** and **General features**: **Enforced report management** functional areas.<br>You can assign this role to a security officer and other managers in charge of the IT security in your organization. |
| Vulnerability and patch management administrator | Permits all operations in the **General features**: **Basic functionality** and **System management** (including all features, *except* the **Execute scripts remotely** feature) functional areas. |
| Vulnerability and patch management operator | Grants the **Read** and **Execute** (where applicable) rights in the **General features**: **Basic functionality** and **System management** (including all features, *except* the **Execute scripts remotely** feature) functional areas. |

# Assigning access rights to specific objects

In addition to assigning access rights at the server level, you can configure access to specific objects, for example, to a specific task. The application allows you to specify access rights to the following object types:

- Administration groups
- Tasks
- Reports
- Device selections
- Event selections

*To assign access rights to a specific object:*

1. Depending on the object type, in the main menu, go to the corresponding section:
   - **Asset management → Hierarchy of groups**
   - **Tasks**
   - **Monitoring → Reports**

- **Asset management → Device selections**
- **Monitoring → Event selections**

2. Open the properties of the object to which you want to configure access rights.

   To open the properties window of an administration group or a task, click the object name. Properties of other objects can be opened by using the button on the toolbar.

3. In the properties window, open the **Access rights** section.

   The user list opens. The listed users and security groups have access rights to the object. By default, if you use a hierarchy of administration groups or Servers, the list and access rights are inherited from the parent administration group or primary Server.

4. To be able to modify the list, enable the **Use custom permissions** option.

5. Configure access rights:

   - Use the **Add** and **Delete** buttons to modify the list.
   - Specify access rights for a user or security group. Do one of the following:
     - If you want to specify access rights manually, select the user or security group, click the **Access rights** button, and then specify the access rights.
     - If you want to assign a user role to the user or security group, select the user or security group, click the **Roles** button, and then select the role to assign.

6. Click the **Save** button.

The access rights to the object are configured.

# Assigning access rights to users and security groups

You can give users and security groups access rights to use different features of Administration Server, for example, Kaspersky Endpoint Security for Linux.

*To assign access rights to a user or a security group:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **Access rights** tab, select the check box next to the name of the user or the security group to whom to assign rights, and then click the **Access rights** button.

   You cannot select multiple users or security groups at the same time. If you select more than one item, the **Access rights** button will be disabled.

3. Configure the set of rights for the user or group:

   a. Expand the node with features of Administration Server or other Kaspersky application.

   b. Select the **Allow** or **Deny** check box next to the feature or the access right that you want.

*Example 1:* Select the **Allow** check box next to the **Application integration** node to grant all available access rights to the Application integration feature (**Read**, **Write**, and **Execute**) for a user or group.

*Example 2:* Expand the **Encryption key management** node, and then select the **Allow** check box next to the **Write** permission to grant the **Write** access right to the Encryption key management feature for a user or group.

4. After you configure the set of access rights, click **OK**.

The set of rights for the user or group of users will be configured.

The permissions of the Administration Server (or the administration group) are divided into the following areas:

- General features:
  - Management of administration groups
  - Access objects regardless of their ACLs
  - Basic functionality
  - Deleted objects
  - Encryption Key Management
  - Event processing
  - Operations on Administration Server (only in the property window of Administration Server)
  - Device tags
  - Kaspersky application deployment
  - License key management
  - Application integration
  - Enforced report management
  - Hierarchy of Administration Servers
  - User permissions
  - Virtual Administration Servers
- Mobile Device Management:
  - General
  - Self Service Portal
- System Management:
  - Connectivity
  - Execute scripts remotely

- Hardware inventory
- Network Access Control
- OS deployment
- Vulnerability and patch management
- Remote installation
- Software inventory

If neither **Allow** nor **Deny** is selected for a permission, then the permission is considered *undefined*: it is denied until it is explicitly denied or allowed for the user.

The rights of a user are the sum of the following:

- User's own rights
- Rights of all the roles assigned to this user
- Rights of all the security group to which the user belongs
- Rights of all the roles assigned to the security groups to which the user belongs

If at least one of these sets of rights has **Deny** for a permission, then the user is denied this permission, even if other sets allow it or leave it undefined.

You can also add users and security groups to the scope of a user role to use different features of Administration Server. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.

# Adding an account of an internal user

If you want to add a user account, ensure that your account has the Modify object ACLs right in the General features: User permissions functional area.

*To add a new internal user account to Kaspersky Security Center Linux:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click **Add**.
3. In the **Add user** window that opens, specify the settings of the new user account:
   - **Name**.
   - **Password** for the user connection to Kaspersky Security Center Linux.

The password must comply with the following rules:

- The password must be 8 to 256 characters long.
- The password must contain characters from at least three of the groups listed below:
  - Uppercase letters (A–Z)
  - Lowercase letters (a-z)
  - Numbers (0–9)
  - Special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- The password may not contain any whitespace, Unicode characters, or the combination of "." and "@" with the "." preceding the "@".

To see the entered password, click .

You can enable the **User must change password at first sign-in** option to force the password change at the first user authentication.

4. Save the changes to complete the creation of the new user account.

A new user account is added to the user list.

To sign in with a created internal user account on the Kaspersky Security Center Web Console, you must assign a role to the account. Before signing in, make sure that the internal user account has a role. Otherwise, a login error will occur.

# Creating a security group

*To create a security group:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Groups** tab.
2. Click the **Add** button.
3. In the **Create security group** window that opens, specify the following settings for the new security group:
   - **Group name**
   - **Description**
4. Click **Save** to save changes.

A new security group is added to the group list.

# Editing an account of an internal user

If you want to edit a user account, ensure that your account has the Modify object ACLs right in the General features: User permissions functional area.

*To edit an internal user account in Kaspersky Security Center Linux:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the name of the user account that you want to edit.
3. In the user settings window that opens, on the **General** tab, change the settings of the user account:
   - **User account**

     If necessary, switch the toggle button to **Inactive** to prohibit the user from connecting to the application. You can disable an account, for example, after an employee leaves the company.
   - Description
   - **Full name**
   - **Email address**
   - **Main phone**
   - **Password**

     If necessary, you can set a new password for the user connection to Kaspersky Security Center Linux as follows:

     a. Click the **Change password** button, and then set a new password for the user account.

     The password must comply with the following rules:

     - The password must be 8 to 256 characters long.
     - The password must contain characters from at least three of the groups listed below:
       - Uppercase letters (A–Z)
       - Lowercase letters (a-z)
       - Numbers (0–9)
       - Special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - The password may not contain any whitespace, Unicode characters, or the combination of "." and "@" with the "." preceding the "@".

     To see the entered password, click .

b. If necessary, enable the **User must change password at first sign-in** option, to force the password change at the next user authentication.

c. If the user account is protected against unauthorized modification, you must confirm that you have the permissions to change this account. In the **Account protection** window, specify the credentials of the account that has the Modify object ACLs right in the General features: User permissions functional area.

4. On the **Two-factor authentication** tab, you can specify the security settings for this account.
5. On the **Groups** tab, you can add the user to security groups.
6. On the **Devices** tab, you can assign devices to the user.
7. On the **Roles** tab, you can assign roles to the user.
8. Save the changes to complete the editing of the user account.

The updated user account appears in the list of users.

# Editing a security group

*To edit a security group:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Groups** tab.
2. Click the name of the security group that you want to edit.
3. In the group settings window that opens, change the settings of the security group:
   - On the **General** tab, you can change the **Name** and **Description** settings. These settings are available only for internal security groups.
   - On the **Users** tab, you can add users to the security group. This setting is available only for internal users and internal security groups.
   - On the **Roles** tab, you can assign a role to the security group.
4. Click **Save** to save changes.

The changes are applied to the security group.

# Assigning a role to a user or a security group

*To assign a role to a user or a security group:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** or the **Groups** tab.
2. Select the name of the user or the security group to whom to assign a role.

   You can select multiple names.

3. On the menu line, click the **Assign role** button.

   The Role assignment wizard starts.

4. Follow the instructions of the wizard: select the role that you want to assign to the selected users or security groups, and then select the scope of role.

   A *user role scope* is a combination of users and administration groups. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.

The role with a set of rights for working with Administration Server is assigned to the user (or users, or the security group). In the list of users or security groups, a check box appears in the **Has assigned roles** column.

# Adding user accounts to an internal security group

You can add only accounts of internal users to an internal security group.

*To add user accounts to an internal security group:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Select check boxes next to user accounts that you want to add to a security group.
3. Click the **Assign group** button.
4. In the **Assign group** window that opens, select the security group to which you want to add user accounts.
5. Click the **Save** button.

The user accounts are added to the security group. You can also add internal users to a security group by using the group settings.

# Assigning a user as a device owner

For information about assigning a user as a mobile device owner, see Kaspersky Secure Mobility Management Help.

*To assign a user as a device owner:*

1. If you want to assign an owner of a device connected to a virtual Administration Server, first switch to the virtual Administration Server:

   a. In the main menu, click the chevron icon (›) to the right of the current Administration Server name.

   b. Select the required Administration Server.

2. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.

   The user list opens. If you are currently connected to a virtual Administration Server, the list includes users from the current virtual Administration Server and the primary Administration Server.

3. Click the name of the user account that you want to assign as a device owner.

4. In the user settings window that opens, select the **Devices** tab.

5. Click the **Add** button.

6. From the device list, select the device that you want to assign to the user.

7. Click **OK**.

The selected device is added to the list of devices assigned to the user.

You can perform the same operation at **Asset management** → **Managed devices**, by clicking the name of the device that you want to assign, and then clicking the **Manage device owner** link.

# Assigning a user as a device owner during installation of Network Agent

To assign a user as a device owner when installing Network Agent via an installation package, add the variables specified in the table below to the Network Agent installation package settings.

| Variable name | Required | Description | Possible values |
|---|---|---|---|
| KLNAGENT_DEVICEOWNER_REGISTRATION_START | No | Allows running the utility for registering the user as a device owner after installation of Network Agent. If turned off, then the registration as a device owner is not available to a user. | 1—The utility for registering the user as a device owner will start after installation of Network Agent.<br>Other—The utility is not available. |
| KLNAGENT_DEVICEOWNER_LOGIN | No<br>Yes, if you enter the password | Contains the login of a user who will be registered as a device owner. | The user's login as specified in the list of users in Kaspersky Security Center Linux. |
| KLNAGENT_DEVICEOWNER_PASSWORD | No<br>Yes, if you enter the login | Contains the encrypted password of a user who will be registered as a device owner. | The user's password. |

Network Agent will decrypt the specified login and password during installation of Kaspersky Security Center Linux, and the user will be registered as a device owner.

You can also assign a user as a device owner when installing Network Agent in silent mode with a response file.

*To assign a user as a device owner when installing Network Agent in a silent mode with a response file:*

1. Add the KLNAGENT_DEVICEOWNER_REGISTRATION_START parameter to the response file and set it to 1.

   The utility for registering the user as a device owner will start after installation of Network Agent.

2. Enter the login and password in the command line on the client device.

   The user will be assigned as a device owner.

If the user is included in an internal security group, the login must contain the user name.

If the user is included in an Active Directory security group, the login must contain the user name and domain name.

You have to enter the time-based one-time password (TOTP) from the app for two-factor authentication.

# Assigning a user as a Linux device owner after installation of Network Agent

*To allow the user to register as a Linux device owner:*

1. In the Kaspersky Security Center Web Console, go to **Software management** → **Installation packages**.

   The list of installation packages opens.

2. Click on the installation package of Network Agent.

   The properties window of the installation package opens.

3. In the installation package properties window, click **Settings** → **Advanced**.

4. In the **User registration as a device owner (Linux only)** section, turn on the **Allow running the user registration utility after Network Agent installation** option and click **Save**.

The utility for registering the user as a device owner can be run via the command line on the client device.

*To register a user as a Linux device owner on the client device:*

1. Execute the following command in the command line on the client device:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Enter the login and password, if prompted.

   If the login and the password are included in the answer file or installation package of Network Agent, execute the following command in the command line on the client device:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

If the user is included in an internal security group, the login must contain the user name.

If the user is included in an Active Directory security group, the login must contain the user name and domain name.

You have to enter the time-based one-time password (TOTP) from the app for two-factor authentication.

The user will be registered as a device owner.

## Removing a user as a device owner

*To remove a user as a device owner on the client device:*

1. Execute the following command in the command line on the client device:

   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner
   ```

2. Enter the user name and password.

If the user is included in an internal security group, the login must contain the user name.

If the user is included in an Active Directory security group, the login must contain the user name and domain name.

You have to enter the time-based one-time password (TOTP) from the app for two-factor authentication.

The user will be removed as the device owner.

# Enabling account protection from unauthorized modification

You can enable an additional option to protect a user account from unauthorized modification. If this option is enabled, modifying user account settings requires authorization of the user with the rights for modification.

*To enable or disable account protection from unauthorized modification:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the name of the internal user account for which you want to specify account protection from unauthorized modification.
3. In the user settings window that opens, select the **Two-factor authentication** tab.
4. On the **Two-factor authentication** tab, select the **Request authentication to verify permission to modify user accounts** option if you want to request credentials and one-time security code for two-factor authentication every time when account settings are changed or modified. Otherwise, select the **Allow users to modify this account without additional authentication** option.
5. Save your changes.

# Configuring two-factor authentication

Starting with Administration Server version 16.1, two-factor authentication is enabled automatically. The global option to disable two-factor authentication is not supported. This scenario provides steps to configure two-step authentication at first sign-in and configure two-factor authentication settings on Administration Server.

## Stages

Configuring two-factor authentication proceeds in stages:

1. **Installing an authenticator app on a device**

   You can install any application that supports the Time-Based One-Time Password algorithm (TOTP).

   Available in Russia:

   - Kaspersky Password Manager for Business (recommended)
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator
   - Aladdin 2FA
   - Rutoken OTP

   Available worldwide (including Russia):

   - Google Authenticator
   - Microsoft Authenticator

   To check if Kaspersky Security Center Linux supports the authenticator app that you want to use, enable two-factor authentication for all users or for a particular user.

   One of the steps suggests that you specify the security code generated by the authenticator app. If it succeeds, then Kaspersky Security Center Linux supports the selected authenticator.

   > We strongly do not recommend installing the authenticator app on the same device from which Administration Server is managed.

2. **Synchronizing the time on the device with the authenticator app with the time of the device on which Administration Server is installed**

   Ensure that the time on the device with the authenticator app and the time on the device with the Administration Server are synchronized to UTC. For better accuracy, we recommend using the same NTP servers throughout your infrastructure. Otherwise, failures may occur while configuring two-factor authentication.

3. **Configuring two-factor authentication for user accounts at sign-in to Web Console**

   Sign-in to Web Console and configure two-factor authentication.

   If two-factor authentication configuration is not available to you, contact a user who has the Modify object ACLs right of the **General features: User permissions** functional area and configured two-factor authentication to add your account to the two-factor authentication allow list.

4. **Configuring two-factor authentication settings on Administration Server**

If you have configured two-factor authentication and the Modify object ACLs right of the **General features**: **User permissions** functional area, you can configure two-factor authentication settings on Administration Server as follows:

1. Reviewing the list of users who can configure two-step authentication at sign-in:

   - For installing Administration Server 16.1 from scratch: Add required users to the two-factor authentication allow list to enable them to configure two-factor authentication at his or her first sign-in.

   - For upgrading or restoring to Administration Server 16.1: Review the two-factor authentication allow list and delete accounts that must not have access to Administration Server.

2. Excluding user accounts for which you do not need to enable two-factor authentication (optional)

   Exclude user accounts from two-factor authentication to allow them to sign in to Administration Server even if they have not configured two-factor authentication. Excluding accounts from two-factor authentication may be necessary for integration accounts that cannot provide a security code during authentication. Integration accounts are used to run scripts through OpenAPI.

3. Resetting or deleting a two-factor authentication secret key (optional)

   You can reset a two-factor authentication secret key when a user loses access to his or her two-factor authentication device, or needs to set up two-factor authentication on a new device. You can also reset a secret key for your own account.

   You can delete a secret key to completely block a user from signing in to Web Console and prevent the user from accessing Administration Server.

4. Editing the name of a security code issuer (optional)

   If you have several Administration Servers with similar names, you may have to change the security code issuer names so there is better recognition of different Administration Servers.

### Results

Upon completion of this scenario:

- Two-factor authentication is configured for your own account and for another user account who needs access to Administration Server.
- Integration accounts are excluded from two-factor authentication.

# About two-factor authentication for an account

Kaspersky Security Center Linux provides two-factor authentication for users of Kaspersky Security Center Web Console. Two-factor authentication is based on the RFC 6238 standard (TOTP: Time-Based One-Time Password algorithm).

Every time you log in to Kaspersky Security Center Web Console, you enter your user name, password, and an additional one-time security code. To receive a one-time security code, you must have an authenticator app on the mobile device or computer.

Any authentication software that supports the Time-Based One-Time Password algorithm (TOTP) can be used as an authenticator app, for example, Google Authenticator. In order to generate the one-time security code, you must synchronize the time set on the device with the authenticator app with the time set on the Administration Server device. For better accuracy, we recommend using the same NTP servers throughout your infrastructure.

To check if Kaspersky Security Center Linux supports the authenticator app that you want to use, try configuring two-factor authentication with this authenticator app.

One of the steps suggests that you specify the one-time security code generated by the authenticator app. If it succeeds, then Kaspersky Security Center Linux supports the selected authenticator.

**Generating a secret code by using an authentication app**

An authenticator app generates the security code as follows:

1. Administration Server generates a special secret key and QR code.
2. You pass the generated secret key or QR code to the authenticator app.
3. The authenticator app generates a single-use security code that you pass to the authentication window of Administration Server.

A security code has an identifier referred to as *issuer name*. The security code issuer name is used as an identifier of the Administration Server in the authenticator app. You can change the name of the security code issuer name. The security code issuer name has a default value that is the same as the name of the Administration Server. A new security code issuer name is assigned to Administration Server after the next sign-in. A security code is single-use and valid for up to 30 seconds (the exact time may vary).

We highly recommend that you save the secret key (or QR code) and keep it in a safe place. This will help you to restore access to Kaspersky Security Center Web Console in case you lose access to the device with the authenticator app.

Two-factor authentication has the following features:

- Starting with Administration Server version 16.1, two-factor authentication is enabled automatically and the option to configure two-factor authentication at sign-in is disabled by default. Configuring two-factor authentication at sign-in is available only to users who are included in the two-factor authentication allowlist.
- A user can configure two-factor authentication only for his or her own account.
- A user can exclude accounts from two-factor authentication. This can be necessary for integration accounts that cannot receive a one-time security code for authentication. Integration accounts are used to run scripts through OpenAPI.
- To regenerate a two-factor authentication secret key, a user must reset the secret key for his or her own account.

- To reset or delete a two-factor authentication secret key for account of another user, a user must have an account with configured two-factor authentication and with the Modify object ACLs right in the **General features**: **User permissions** functional area.
- To exclude accounts of other users from two-factor authentication or modify the two-factor authentication allowlist, a user must have an account with configured two-factor authentication and with the Modify object ACLs right in the **General features**: **User permissions** functional area.
- There should always be at least one user with configured two-factor authentication so that this user can manage the two-factor authentication allowlist and the exclusion list.
- Two-factor authentication is enabled automatically only for Administration Server version 16.1. If other primary or secondary Administration Servers are running version 16 or earlier, their two-factor authentication settings will remain unchanged.
- A virtual Administration Server inherits two-factor authentication settings from the physical Administration Server so that if two-factor authentication is enabled on the physical Administration Server, it is also enabled on a virtual Administration Server. You cannot configure two-factor authentication settings on a virtual Administration Server.
- For two-factor authentication to function correctly, you need to upgrade the Administration Server and Web Console to version 16.1 or later.

To ensure comprehensive protection by using two-factor authentication, it is necessary to secure not only Administration Server but also the device on which it is installed. To do this, consider the Hardening guide recommendations.

# Configuring a two-factor authentication secret key at Kaspersky Security Center Web Console sign-in

The first time you sign in to Kaspersky Security Center Linux 16.1 or later, the window for configuring two-factor authentication opens.

*To configure two-factor authentication for your account:*

1. Install any application that supports the Time-Based One-Time Password algorithm (TOTP) on the mobile device or computer.

   Available in Russia:

   - Kaspersky Password Manager for Business (recommended)
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator
   - Aladdin 2FA
   - Rutoken OTP

Available worldwide (including Russia):

- Google Authenticator
- Microsoft Authenticator

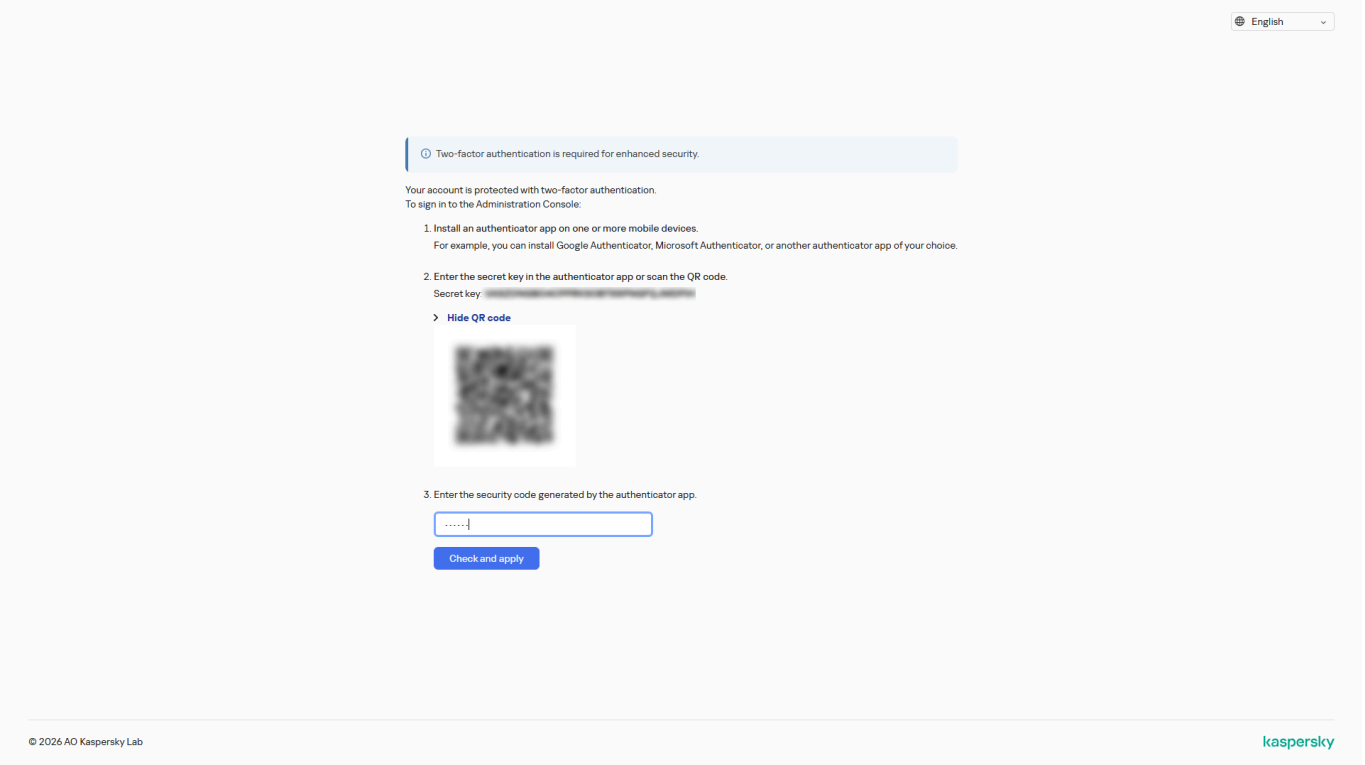
> We strongly do not recommend installing the authenticator app on the same device from which Administration Server is managed.

2. Ensure that the time on the device with the authenticator app and the time on the device with the Administration Server are synchronized to UTC. For better accuracy, we recommend using the same NTP servers throughout your infrastructure.

3. Generate a one-time security code by using the authenticator app on the mobile device or computer. To do so, follow one of these steps:

   - Enter the two-factor authentication secret key in the authenticator app manually.
   - Click **View QR code** and scan the QR code by using the authenticator app.

   A one-time security code of 6 digits will display on the mobile device.




Configuring a two-factor authentication secret key at Kaspersky Security Center Web Console sign-in

4. In the **Two-factor authentication** window, specify the one-time security code generated by the authenticator app, and then click the **Check and apply** button.

   **Rutoken OTP configuration**

   If you use Rutoken OTP, you need an Android mobile device with the Rutoken OTP application installed. The Android mobile device must the following requirements:

   - Operating system is Android 7 or newer.
   - NFC module is available and enabled.

In the Rutoken OTP application, you have to configure the following parameters:

- Scan the QR code displayed in the two-step configuration wizard.
- Set the time interval to 30 seconds.
- Select SHA1 as the algorithm.

*To configure Rutoken OTP:*

1. Put the Rutoken OTP device next to the mobile device with the NFC module.
2. In the Rutoken OTP application, press **Connect token**.
3. In the Rutoken OTP application, press **Configure settings**, and then press **Save secret key.**

   If the token is successfully connected to the mobile device, the Rutoken OTP application shows the following status messages:

   - **Token is connected.**
   - **Settings are configured.**
   - **Secret key is saved.**
4. On the Rutoken OTP device, press the button.

   A security code is displayed on the device.
5. In Kaspersky Security Center Web Console, in the two-step verification window, enter the security code.

Two-factor authentication is configured for your account. You are able to access the Administration Server in accordance with your rights.

If two-factor authentication configuration is not available to you, contact a user who has the Modify object ACLs right in the **General features**: **User permissions** functional area and configured two-factor authentication to add your account to the two-factor authentication allowlist.

# Allowing users to configure two-factor authentication

The two-factor authentication allowlist is a list of users who are permitted to initially configure two-factor authentication when signing in to Web Console. This list contains user accounts without configured two-factor authentication. By default, new user accounts are not included in the two-factor authentication allowlist and must be added to the list by an administrator. If a new account is an integration account used to run OpenAPI scripts, it must be excluded from two-factor authentication.

A user account will be automatically deleted from the two-factor authentication allowlist when it has configured two-factor authentication or is excluded from two-factor authentication.

Manual modifying the two-factor authentication allowlist is available for accounts that have configured two-factor authentication and that have the Modify object ACLs right in the **General features**: **User permissions** functional area.

*To add a user account to the two-factor authentication allowlist manually:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **Two-factor authentication** tab of the properties window, in the **Users allowed to generate secret keys** table, click the **Add** button.

3. In the window that opens:

   a. Select the user account that you want to add.

      Only users who are not excluded from two-factor authentication and do not have a two-factor authentication secret key can be added to the two-factor authentication allowlist.

   b. If the account is protected against unauthorized modification, you must confirm that you have the permissions to change this account. In the **Account protection** window, specify the credentials of your own account and the one-time security code for two-factor authentication.

   c. Save your changes.

The selected user account is added to the two-factor authentication allowlist. At the next sign-in, the user will be able to generate a secret key.

A user account can be deleted from the two-factor authentication allowlist until two-factor authentication is configured for that account.

*To delete user accounts from the two-factor authentication allowlist manually:*

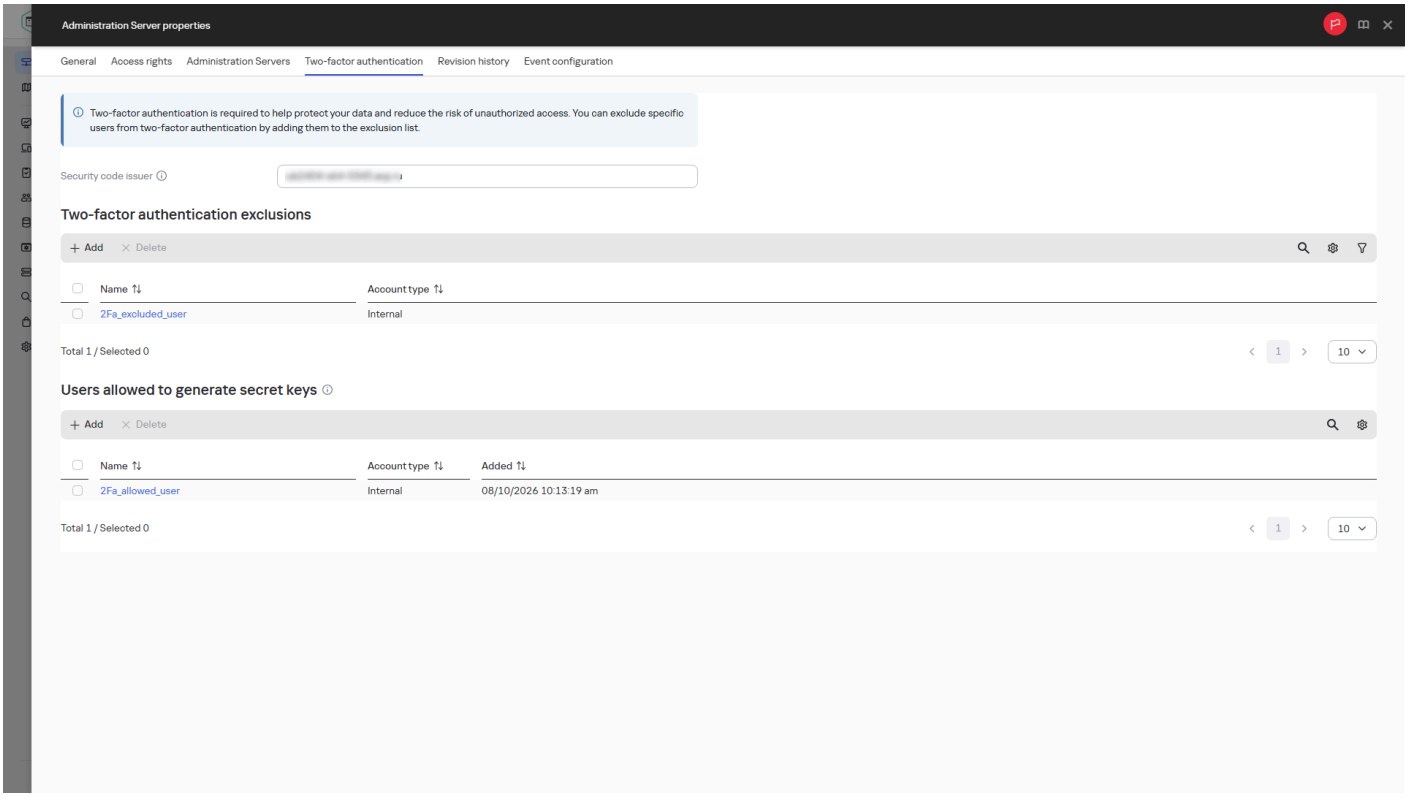
1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **Two-factor authentication** tab of the properties window, in the **Users allowed to generate secret keys** table, select the user accounts that you want to delete, and then click **Delete**.

3. If the account is protected against unauthorized modification, you must confirm that you have the permissions to change this account. In the **Account protection** window, specify the credentials of your own account and the one-time security code for two-factor authentication.

The selected user accounts are deleted from the two-factor authentication allowlist.




Configuring the two-factor authentication allowlist

If, during an active session on Administration Server, your two-factor authentication secret key is deleted by another user or you reset the key yourself but do not create a new one, the ability to modify the two-factor authentication allowlist is blocked.

User accounts can also be automatically added and deleted from the two-factor authentication allowlist.

When resetting a two-factor authentication secret key for other accounts, their accounts are automatically added to the two-factor authentication allowlist so that they can generate a new secret key.

When upgrading Administration Server from version 16 or earlier to version 16.1 or later, as well as when you create a data backup on Administration Server 16 or earlier and restore it on Administration Server 16.1 or later, user accounts will be automatically added to the two-factor authentication allowlist if all the following conditions are met:

- User has the Read permission in the functional area *General features: Basic functionality* assigned directly to the user (not through a security group). The scope of the user role with this permission must include all managed and unassigned devices, and must be set at the Administration Server level.
- User is not excluded from two-factor authentication.
- User does not have a two-factor authentication secret key.
- Two-factor authentication was not enabled for all users on Administration Server of the previous version.

Failure to meet even one condition will result in the user not being added to the two-factor authentication allowlist.

> After an upgrade or restore, we recommend ensuring that the two-factor authentication allowlist contains only the user accounts that must have access to Administration Server. Review the two-factor authentication allowlist and remove any other accounts from it. Add integration accounts used to run scripts through OpenAPI to the exclusion list to prevent script failures.

Accounts of the users will lose access to Administration Server after an upgrade or restore if all the following conditions are met:

- User has the Read permission in the functional area *General features: Basic functionality* assigned through a security group (not directly to the user) or does not have this permission at all.
- User is not excluded from two-factor authentication.
- User does not have a two-factor authentication secret key.
- Two-factor authentication was not enabled for all users on Administration Server of the previous version.

These accounts can be manually added to the two-factor authentication allowlist, if needed.

# Resetting and deleting a two-factor authentication secret key

You can reset a secret key when a user loses access to his or her two-factor authentication device or needs to set up two-factor authentication on a new device. Resetting the secret key allows the user to sign in to Web Console again and generate a new secret key.

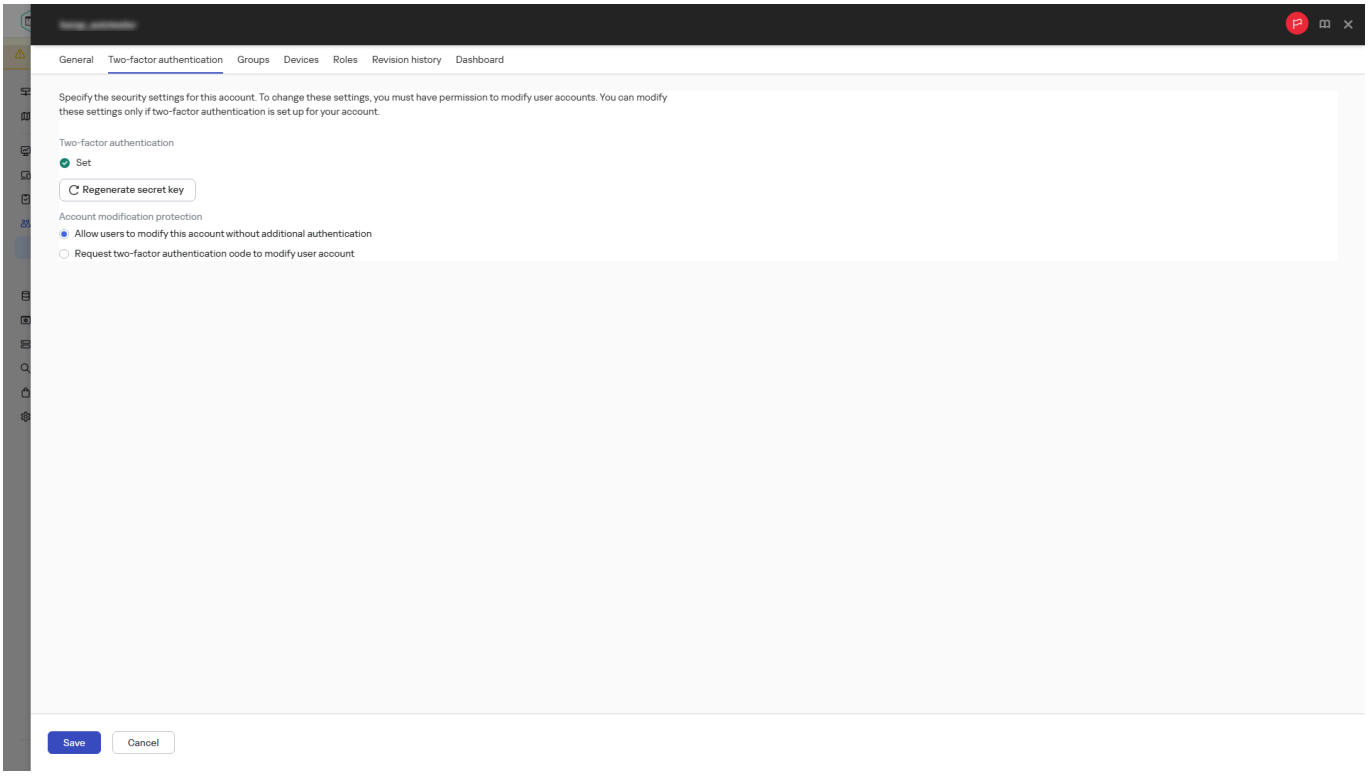
> You can reset or delete a two-factor authentication secret key for accounts of other users only if you have configured two-factor authentication and you have the Modify object ACLs right in the **General features**: **User permissions** functional area. You can also regenerate your own secret key.

*To reset a secret key for an account:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the name of the user account for which you want to reset a secret key.

3. If you want to reset a secret key for your account:

a. On the **Two-factor authentication** tab, click the **Regenerate secret key** button.

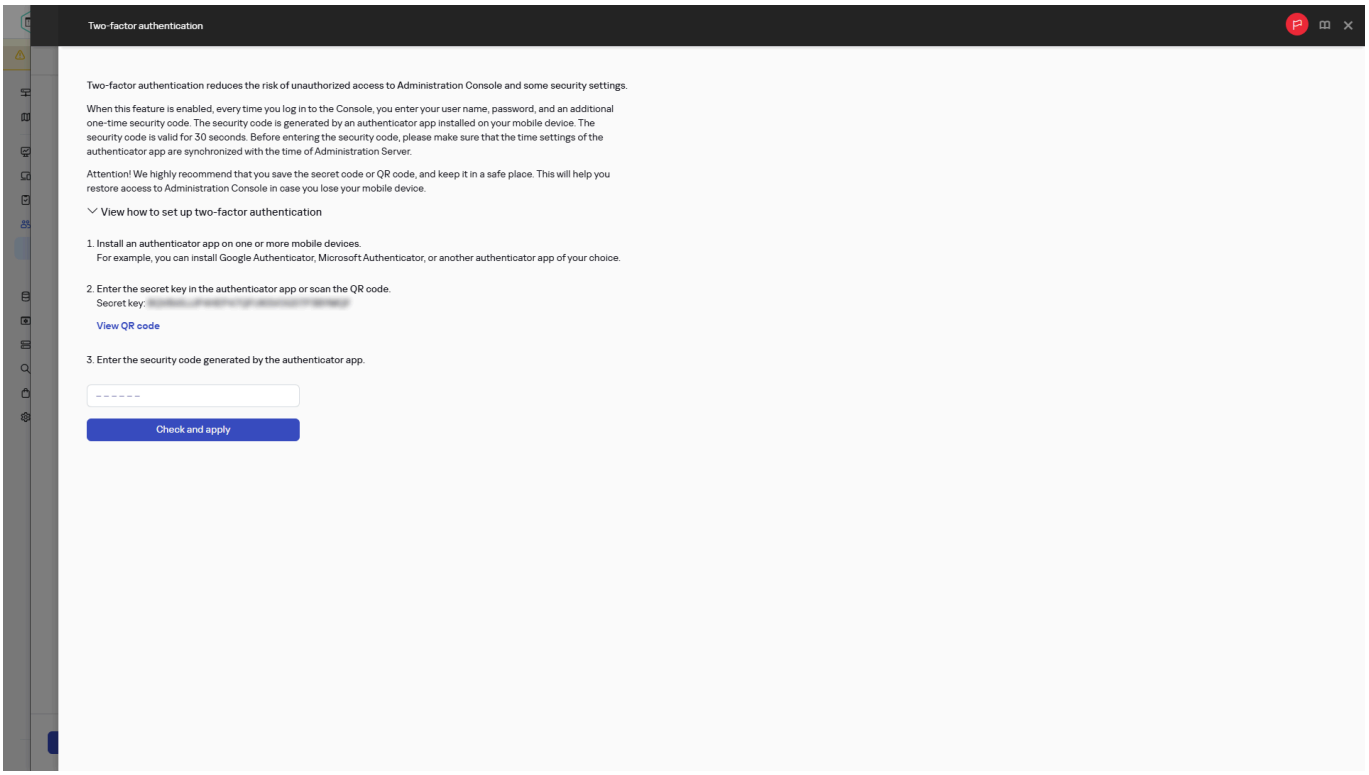



Regenerating the two-factor authentication secret key for the current user account

a. If your account is protected against unauthorized modification, you must confirm that you have the permissions to change this account. In the **Account protection** window, specify the credentials of your own account and the two-factor authentication code.

b. In the **Two-factor authentication** window, click **View how to set up two-factor authentication**, and then click **View QR code**.

c. Use the authenticator app on the mobile device to scan the QR code and receive a one-time security code.




Configuring a new two-factor authentication secret key for the current user account

a. In the **Two-factor authentication** window, specify the one-time security code generated by the authenticator app, click the **Check and apply** button, and then save changes.

**Rutoken OTP configuration**

If you use Rutoken OTP, you need an Android mobile device with the Rutoken OTP application installed. The Android mobile device must the following requirements:

- Operating system is Android 7 or newer.
- NFC module is available and enabled.

In the Rutoken OTP application, you have to configure the following parameters:

- Scan the QR code displayed in the two-step configuration wizard.
- Set the time interval to 30 seconds.
- Select SHA1 as the algorithm.

*To configure Rutoken OTP:*

1. Put the Rutoken OTP device next to the mobile device with the NFC module.
2. In the Rutoken OTP application, press **Connect token**.
3. In the Rutoken OTP application, press **Configure settings**, and then press **Save secret key.**

If the token is successfully connected to the mobile device, the Rutoken OTP application shows the following status messages:

- **Token is connected.**
- **Settings are configured.**
- **Secret key is saved.**

4. On the Rutoken OTP device, press the button.

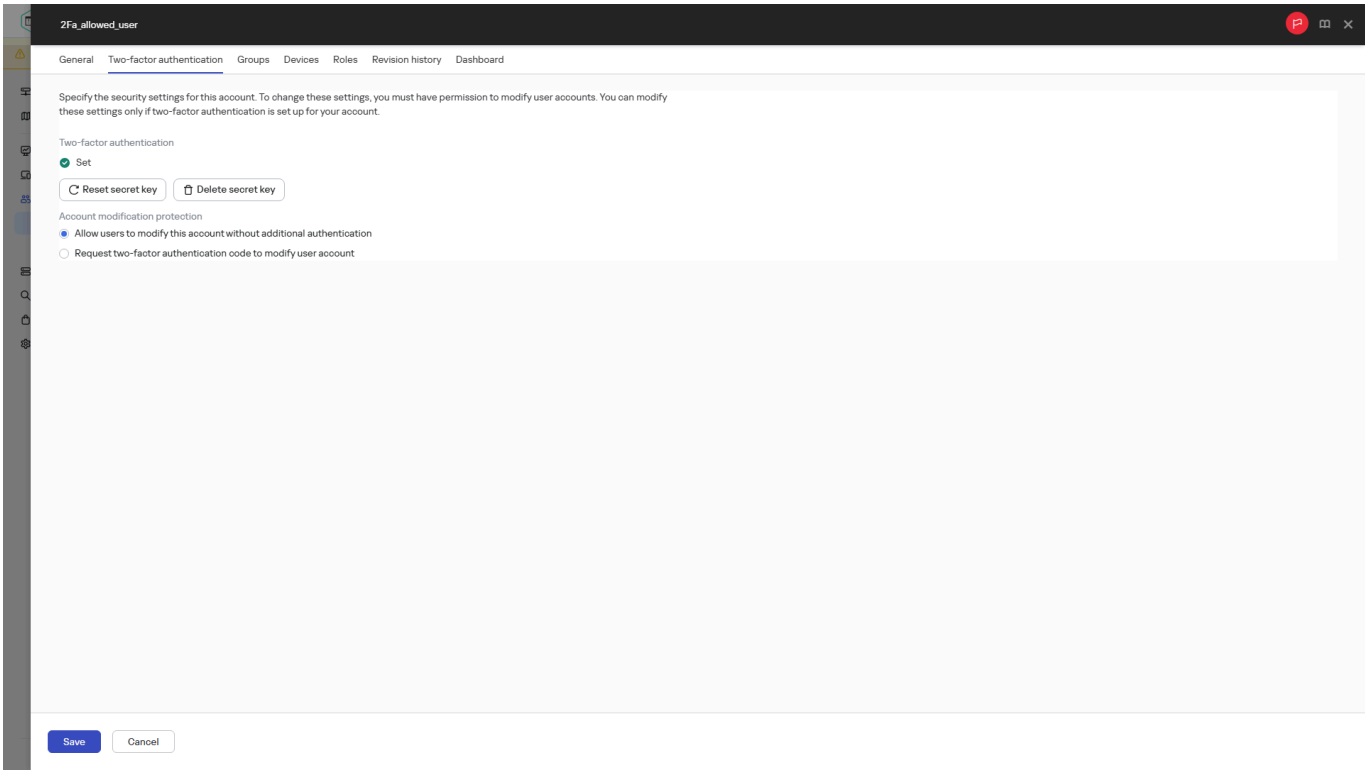
   A security code is displayed on the device.

5. In Kaspersky Security Center Web Console, in the two-step verification window, enter the security code.

The secret key for your account is changed.

4. If you want to reset a secret key for another account:

   a. On the **Two-factor authentication** tab, click the **Reset secret key** button.




Resetting the two-factor authentication secret key for another user account

   a. If the account is protected against unauthorized modification, you must confirm that you have the permissions to change this account. In the **Account protection** window, specify the credentials of your own account and the one-time security code for two-factor authentication.

   b. Confirm the reset of the secret key, and then save changes.

When you reset a secret key for another account, the existing secret key is deleted and the user account is added to the two-factor authentication allowlist in the Administration Server properties. At the next sign-in, the user will be able to generate a new secret key.

The secret key of a user account is reset.

You can delete a secret key to completely block a user from signing in to Web Console and prevent the user from accessing Administration Server.

*To delete a secret key:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the name of the internal user account for which you want to delete a secret key.

   You cannot delete a secret key for your own account.

3. On the **Two-factor authentication** tab, click the **Delete secret key** button.
4. If the account is protected against unauthorized modification, you must confirm that you have the permissions to change this account. In the **Account protection** window, specify the credentials of your own account and the one-time security code for two-factor authentication.
5. Confirm the deletion of the secret key, and then save changes.

The secret key of a user account is deleted.

You can restore access by adding the user to the two-factor authentication allowlist in the Administration Server properties. In this case, at the next sign-in, the user will be able to generate a new secret key.

# Excluding accounts from two-factor authentication

You can exclude user accounts from two-factor authentication to allow them to sign in to Administration Server even if they have not configured two-factor authentication. Excluding accounts from two-factor authentication may be necessary for integration accounts that cannot provide a one-time security code during authentication. Integration accounts are used to run scripts through OpenAPI.

You can modify the exclusion list if two-factor authentication is configured for your account and you have the Modify object ACLs right in the **General features**: **User permissions** functional area.

*To exclude a user account from two-factor authentication:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **Two-factor authentication** tab of the properties window, in the **Two-factor authentication exclusions** table, click the **Add** button.

3. In the window that opens:

   a. Select the user account that you want to exclude.

   b. If the account is protected against unauthorized modification, you must confirm that you have the permissions to change this account. In the **Account protection** window, specify the credentials of your own account and the one-time security code for two-factor authentication.

   c. Save your changes.

The selected user accounts are excluded from two-factor authentication, and their secret keys are deleted if they exist. The list of excluded accounts is not changed when you restore a backup on Administration Server 16.1, or upgrade Administration Server to version 16.1 or later. If the accounts from the exclusion list had secrets in the previous version of the Administration Server, these secret keys will be deleted in 16.1.

You can delete user accounts from the exclusion list to completely block users from signing in to Web Console and to prevent users from accessing Administration Server.

*To delete user accounts from the exclusion list:*

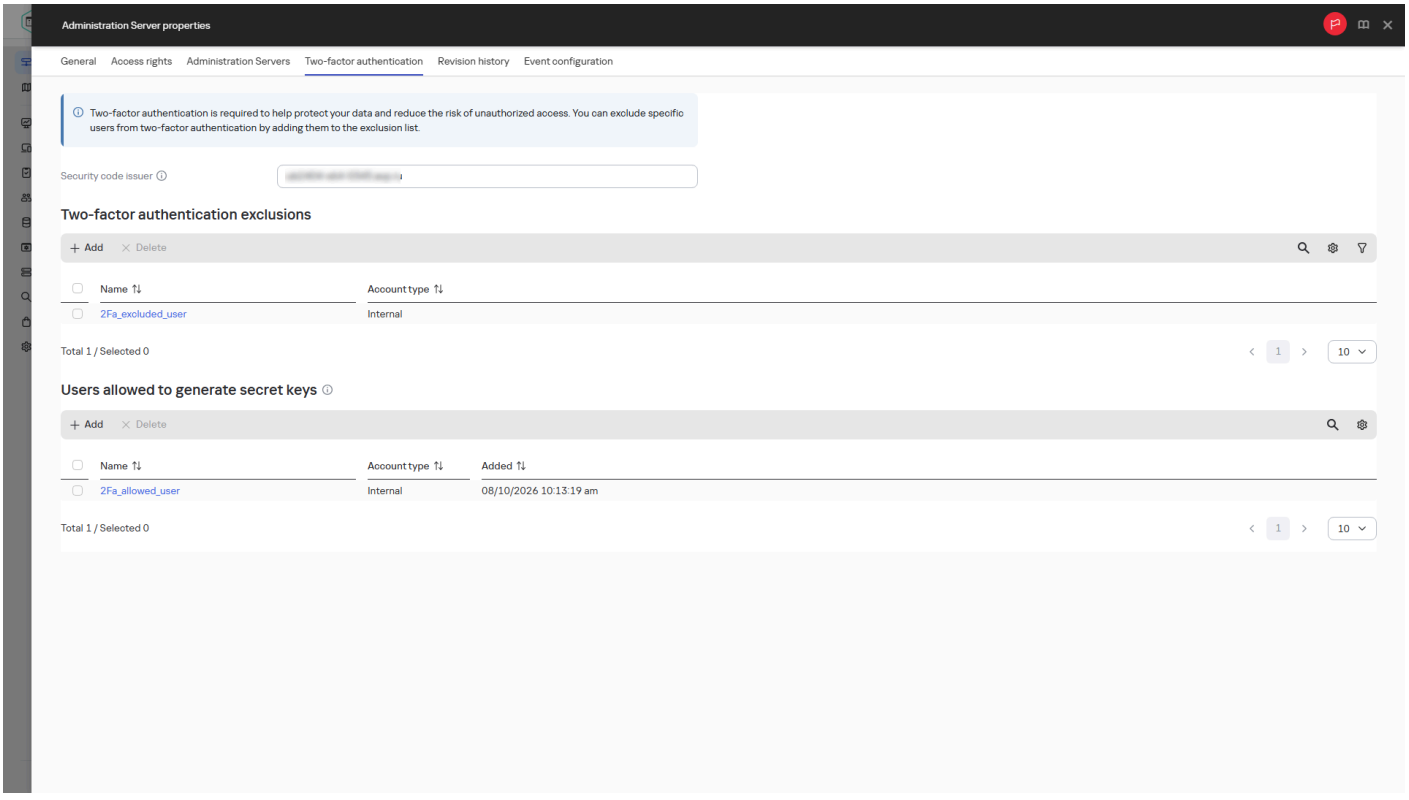
1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **Two-factor authentication** tab of the properties window, in the **Two-factor authentication exclusions** table, select the user accounts that you want to delete, and then click **Delete**.

3. If the account is protected against unauthorized modification, you must confirm that you have the permissions to change this account. In the **Account protection** window, specify the credentials of your own account and the one-time security code for two-factor authentication.

The selected user accounts are deleted from the exclusion list.




Configuring the two-factor authentication exclusion list

# Editing the name of a security code issuer

You can have several identifiers (called issuers) for different Administration Servers. You can change the name of a security code issuer in case, for example, the Administration Server already uses a similar name of the security code issuer for another Administration Server. By default, the name of a security code issuer is the same as the name of the Administration Server.

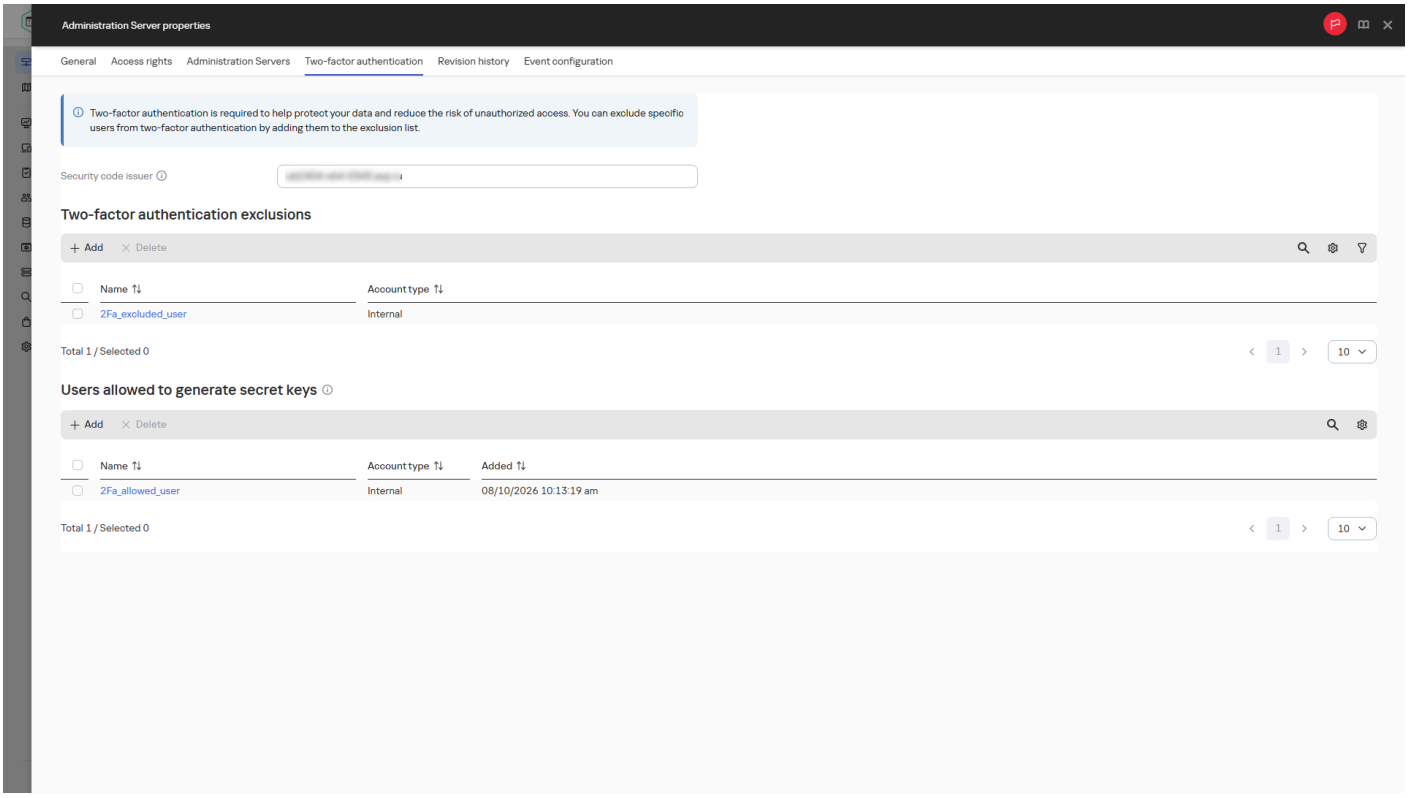
*To specify a new name of a security code issuer:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **Two-factor authentication** tab of the properties window, enter a new name in the **Security code issuer** field, and then save changes.

A new security code issuer name is assigned to Administration Server after the next sign-in.




Specifying the name of a security code issuer

# Changing the number of allowed password entry attempts

The Kaspersky Security Center Linux user can enter an invalid password a limited number of times. After the limit is reached, the user account is blocked for one hour.

By default, the maximum number of allowed password entry attempts is 10. You can change the number of allowed password entry attempts, as described in this section.

*To change the number of allowed password entry attempts:*

1. On the Administration Server device, run a Linux command line.
2. For the klscflag utility, run the following command:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   where N is a number of attempts to enter a password.
3. To apply the changes, restart the Administration Server service.

The maximum number of allowed password entry attempts is changed.

# Deleting a user or a security group

You can delete only internal users or internal security groups.

*To delete a user or a security group:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** or the **Groups** tab.
2. Select the check box next to the user or the security group that you want to delete.

   There should always be at least one user with configured two-factor authentication so that this user can manage the two-factor authentication allowlist and the exclusion list.
3. Then click the **Delete** button.
4. In the window that opens, click **OK**.

The user or the security group is deleted.

# Changing a user account password

You may need to change the password for your own account or for other user account if the current password is about to expire or you want to change it to a more secure one.

The password must comply with the following rules:

- The password must be 8 to 256 characters long.
- The password must contain characters from at least three of the groups listed below:
  - Uppercase letters (A–Z)
  - Lowercase letters (a-z)
  - Numbers (0–9)
  - Special characters (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- The password may not contain any whitespace, Unicode characters, or the combination of "." and "@" with the "." preceding the "@".

## Changing your account password

*To edit the password for your account:*

1. In the upper pane, go to your account menu by clicking your account name.
2. From the drop-down list, select **Change password**.
3. In the right pane that opens, enter the current password, and then specify the new password for the connection to Kaspersky Security Center Linux.

   To see the entered password, click .
4. If your account is protected against unauthorized modification, you must confirm that you have the permissions to change this account. In the **Account protection** window, specify the credentials of your own account or the account that has the Modify object ACLs right in the **General features**: **User permissions** functional area.
5. Enter the one-time security code generated by the authenticator app on the mobile device.

## Changing the password for an internal user account

*To edit the password for an internal user account:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the name of the user account that you want to edit.
3. In the user settings window that opens, on the **General** tab, click the **Change password** button.
4. Set a new password for the user connection to Kaspersky Security Center Linux.

   To see the entered password, click .

5. If necessary, enable the **User must change password at first sign-in** option, to force the password change at the next user authentication.

6. If the user account is protected against unauthorized modification, you must confirm that you have the permissions to change this account. In the **Account protection** window, specify the credentials of the account that has the Modify object ACLs right in the **General features**: **User permissions** functional area.

7. Enter the one-time security code generated by the authenticator app on the mobile device.

## Configuring the options for changing password by using server flags

Run the command line, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where Network Agent is installed. The default installation directory is `/opt/kaspersky/ksc64/sbin`. Run the following commands:

- Configuring the password rotation period (the `LP_SplPwdChangePeriodDays` flag)

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <rotation_period>`

  Where `<rotation_period>` is a period of time in days after which the user password expires. Possible values: 0–730. If the parameter value is 0, the password rotation is disabled.

- Configuring the time of the preliminary warning about the need to change the password (the `LP_SplPwdChangeNotificationHours` flag)

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <warning_time>`

  Where `<warning_time>` is a period of time in hours before the user password expires. During this time, the notification about the need for the password change is displayed. Possible values: 0–17520. If the parameter value is 0, the warning time is 25 percent of the password rotation period.

- Specifying the default value of the **User must change password at first sign-in** option (the `LP_SplPwdForceChange` flag)

  `./klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <value>`

  Where the possible values of the `<value>` flag:

  `1`—the **User must change password at first sign-in** option is enabled.

  `0`—the **User must change password at first sign-in** option is disabled.

To view the current flag value, run the following command:

`./klscflag -fget -pv .core/.independent -s KLLIM -n <flag> -t d`

Where `<flag>` is the `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours`, or `LP_SplPwdForceChange` flag.

# Creating a user role

*To create a user role:*

1. In the main menu, go to **Users & roles** → **Roles**.
2. Click the **Add** button.
3. In the **New role name** window that opens, enter the name of the new role.
4. Click **OK** to apply the changes.
5. In the role properties window that opens, change the settings of the role:
   - On the **General** tab, edit the role name.
     You cannot edit the name of a predefined role.
   - On the **Settings** tab, edit the role scope and policies and profiles associated with the role.
   - On the **Access rights** tab, edit the rights for access to Kaspersky applications.
6. Click **Save** to save changes.

The new role appears in the list of user roles.

# Editing a user role

*To edit a user role:*

1. In the main menu, go to **Users & roles** → **Roles**.
2. Click the name of the role that you want to edit.
3. In the role properties window that opens, change the settings of the role:
   - On the **General** tab, edit the role name.
     You cannot edit the name of a predefined role.
   - On the **Settings** tab, edit the role scope and policies and profiles associated with the role.
   - On the **Access rights** tab, edit the rights for access to Kaspersky applications.
4. Click **Save** to save changes.

The updated role appears in the list of user roles.

# Editing the scope of a user role

A *user role scope* is a combination of users and administration groups. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.

*To add users, security groups, and administration groups to the scope of a user role, you can use either of the following methods:*

*Method 1:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** or the **Groups** tab.
2. Select check boxes next to the users or security groups that you want to add to the user role scope.
3. Click the **Assign role** button.

   The Role assignment wizard starts. Proceed through the wizard by using the **Next** button.
4. On the **Select role** step, select the user role that you want to assign.
5. On the **Define scope** step, select the administration group that you want to add to the user role scope.
6. Click the **Assign role** button to close the window.

The selected users or security groups and the selected administration group are added to the scope of the user role.

*Method 2:*

1. In the main menu, go to **Users & roles** → **Roles**.
2. Click the name of the role for which you want to define the scope.
3. In the role properties window that opens, select the **Settings** tab.
4. In the **Role scope** section, click **Add**.

   The Role assignment wizard starts. Proceed through the wizard by using the **Next** button.
5. On the **Define scope** step, select the administration group that you want to add to the user role scope.
6. On the **Select users** step, select users and security groups that you want to add to the user role scope.
7. Click the **Assign role** button to close the window.
8. Click the **Close** button (×) to close the role properties window.

The selected users or security groups and the selected administration group are added to the scope of the user role.

*Method 3:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **Access rights** tab, select the check box next to the name of the user or the security group that you want to add to the user role scope, and then click the **Roles** button.

   You cannot select multiple users or security groups at the same time. If you select more than one item, the **Roles** button will be disabled.

3. In the **Roles** window, select the user role that you want to assign, and then apply and save changes.

   The selected users or security groups are added to the scope of the user role.

# Deleting a user role

*To delete a user role:*

1. In the main menu, go to **Users & roles** → **Roles**.
2. Select the check box next to the name of the role that you want to delete.
3. Then click the **Delete** button.
4. In the window that opens, click **OK**.

The user role is deleted.

# Associating policy profiles with roles

You can associate user roles with policy profiles. In this case, the activation rule for this policy profile is based on the role: the policy profile becomes active for a user that has the specified role.

For example, the policy bars any GPS navigation software on all devices in an administration group. GPS navigation software is necessary only on a single device in the Users administration group—the device owned by a courier. In this case, you can assign a "Courier" role to its owner, and then create a policy profile allowing GPS navigation software to run only on the devices whose owners are assigned the "Courier" role. All the other policy settings are preserved. Only the user with the role "Courier" will be allowed to run GPS navigation software. Later, if another worker is assigned the "Courier" role, the new worker also can run navigation software on your organization's device. Running GPS navigation software will still be prohibited on other devices in the same administration group.

*To associate a role with a policy profile:*

1. In the main menu, go to **Users & roles** → **Roles**.
2. Click the name of the role that you want to associate with a policy profile.

   The role properties window opens with the **General** tab selected.

3. Select the **Settings** tab, and scroll down to the **Policies** section.

4. Click **Edit**.

5. To associate the role with:

   - **An existing policy profile**—Click the chevron icon (>) next to the required policy name, and then select the check box next to the profile with which you want to associate the role.
   - **A new policy profile**:

     a. Select the check box next to the policy for which you want to create a profile.

     b. Click **New policy profile**.

     c. Specify a name for the new profile and configure the profile settings.

     d. Click the **Save** button.

     e. Select the check box next to the new profile.

6. Click **Assign to role**.

   The profile is associated with the role and appears in the role properties. The profile applies automatically to any device whose owner is assigned the role.

# Propagating user roles to secondary Administration Servers

By default, the lists of user roles of the primary and secondary Administration Servers are independent. You can configure the application to automatically propagate the user roles created on the primary Administration Server to all of the secondary Administration Servers. The user roles can also be propagated from a secondary Administration Server to its own secondary Administration Servers.

*To propagate user roles from the primary Administration Server to the secondary Administration Servers:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens with the **General** tab selected.

2. Go to the **Hierarchy of Administration Servers** section.

3. Enable the **Relay list of roles to secondary Administration Servers** option, and then click the **Save** button.

   The application copies the user roles of the primary Administration Server to the secondary Administration Servers.

When the **Relay list of roles to secondary Administration Servers** option is enabled and the user roles are propagated, they cannot be edited or deleted on the secondary Administration Servers. When you create a new role or edit an existing one on the primary Administration Server, the changes are automatically copied to the secondary Administration Servers. When you delete a user role on the primary Administration Server, this role remains on the secondary Administration Servers afterward, but it can be edited or deleted.

The roles that are propagated to the secondary Administration Server from the primary Server are displayed with green check marks (✓). You cannot edit these roles on the secondary Administration Server.

If you create a role on the primary Administration Server, and there is a role with the same name on its secondary Administration Server, the new role is copied to the secondary Administration Server with the index added to its name, for example, ~~1, ~~2 (the index can be random).

If you disable the **Relay list of roles to secondary Administration Servers** option, all the user roles remain on the secondary Administration Servers, but they become independent from those on the primary Administration Server. After becoming independent, the user roles on the secondary Administration Servers can be edited or deleted.

# Changing account password

You can change the local account password, for example, when the user forgets the local account password or to perform a scheduled password change.

The password change will apply even if the user has not signed in to the account. You can also change the password for the local root account.

This task may be performed only on Linux devices.

*To change the local account password on specific devices:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts.
3. In the **Task type** field, select **Change account password (Linux only)**.
4. Choose one of the following options:

   **Assign task to an administration group**

   The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

   For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

   If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

   **Specify device addresses manually or import addresses from a list**

   You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

   You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

   **Assign task to a device selection**

   The task is assigned to devices included in a device selection. You can specify one of the existing selections.

   For example, you may want to use this option to run a task on devices with a specific operating system version.

   The *Change account password (Linux only)* task is created for the specified devices. If you selected the **Assign task to an administration group** option, the task is a group one.

5. At the **Task scope** step, specify an administration group, devices with specific addresses, or a device selection.

   The available settings depend on the option selected at the previous step.

6. At the **Enter account name and new password** step, specify the following settings:

   - In the **Account name** field, specify the name of the account for which you want to change the password.
   - In the **New password** field, specify the password, that will be set for the account specified in the previous field.

     To see the characters that you entered, click and hold the **Show** button.
   - If necessary, select the **Set as a one-time password (the user must change the password after the first login)** check box.

     **Set as a one-time password (the user must change the password after the first login)**

     If this check box is selected, the user will be prompted to set a new password after the first login.

     If this check box is cleared, the user will not be prompted to set a new password after the first login.

     This check box is cleared by default.

7. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

   If you enabled the **Open task details when creation is complete** option, the task settings window opens. In this window, you can check the task parameters, modify them, or configure a task start schedule, if necessary.

8. In the task list, select the task you created, and then click **Start**.

   Alternatively, wait for the task to launch according to the schedule that you specified in the task settings.

When the change account password task completes, the password is changed for the specified local account on the specified devices.

To ensure correct operation of the change account password tasks, SELinux must be disabled on the user device.

# Revoking local administrator rights

You can revoke local administrator rights from accounts. This provides you with an extra layer of control of user accounts. For example, you can revoke local administrator rights after a one-time assignment is complete.

When this task is run, the specified local account is checked to see whether it belongs to local administrator groups.These groups are defined in the Network Agent policy settings. You may customize the list of local administrator groups in the Network Agent policy settings. You can also check the list of privileged user accounts using the **Report on privileged device users (Linux only)**.

This task may be performed only on Linux devices.

*To revoke local administrator rights on specific devices:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts.
3. In the **Task type** field, select **Revoke local administrator rights (Linux only)**.
4. Choose one of the following options:

   **Assign task to an administration group**

   The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

   For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

   If a task is assigned to an administration group, the **Security** tab is not displayed in the task properties window because group tasks are subject to the security settings of the groups to which they apply.

   **Specify device addresses manually or import addresses from a list**

   You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

   You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

   **Assign task to a device selection**

   The task is assigned to devices included in a device selection. You can specify one of the existing selections.

   For example, you may want to use this option to run a task on devices with a specific operating system version.

   The *Revoke local administrator rights(Linux only)* task is created for the specified devices. If you selected the **Assign task to an administration group** option, the task is a group one.
5. At the **Task scope** step, specify an administration group, devices with specific addresses, or a device selection.

   The available settings depend on the option selected at the previous step.
6. At this step of the wizard, specify the following settings:

   - In the **Operating mode** settings group, select the operating mode:

     **Revoke local administrator rights from listed accounts**

     If this option is selected, local administrator rights will be revoked from the specified local accounts.

     By default, this option is selected.

     **Exclude listed accounts from local administrator rights revocation**

     If this option is selected, local administrator rights will be revoked from all local accounts, except the specified ones.

     By default, this option is not selected.

- Specify the local accounts:
  - Click **Add**.
  - In the window that opens, do one of the following:
    - In the **Account name** field, specify the name of the local account.
    - In the **Account action** settings group (available only if the **Revoke local administrator rights from listed accounts** option is selected), select the action.
    - **Keep account**

      If this option is selected, the local account is not deleted after local administrator rights are revoked.

      By default, this option is selected.
    - **Delete account**

      If this option is selected, the local account will be deleted regardless of whether it has local administrator rights.

      By default, this option is not selected.

7. At the **Finish task creation** step, click the **Finish** button to create the task and close the wizard.

   If you enabled the **Open task details when creation is complete** option, the task settings window opens. In this window, you can check the task parameters, modify them, or configure a task start schedule, if necessary.

8. In the task list, select the task you created, and then click **Start**.

   Alternatively, wait for the task to launch according to the schedule that you specified in the task settings.

When the revoke local administrator rights task is completed, the local administrator rights are revoked from the specified local accounts on the specified devices.

# Configuring Kerberos domain authentication

Kaspersky Security Center Linux enables you to use domain authentication over the Kerberos protocol. Domain authentication allows you to enable secure authentication in Kaspersky Security Center Web Console without having to re-enter the password on the corporate network (single sign-on).

You must first configure your domain controller to use Kerberos and generate a keytab file. For more information, refer to the documentation for your domain controller.

SCRIL (Smart card is required for interactive logon) is supported for Microsoft Active Directory.

## Generating a keytab file for FreeIPA and AldPro

*To generate a keytab file:*

1. Create a user account to be used by IAM to access the domain controller.

2. If the Administration Server is outside the FreeIPA/AldPro domain, add the DNS record entry and the host entry:

   ```
   ipa dnsrecord-add <zoneName> <recordName> --a-rec <Administration Server IP address>
   ipa host-add --password=<password> <Administration Server host address>
   ```

3. Specify the PAC type when creating the HTTP service for the Administration Server:

   ```
   ipa service-add HTTP/<Administration Server host FQDN>@<DOMAIN WRITTEN IN CAPITAL LETTERS> --ok-to-auth-as-delegate=true --pac-type PAD
   ```

4. Specify the user account for authentication:

   ```
   ipa service-allow-retrieve-keytab HTTP/<Administration Server host address>@<DOMAIN WRITTEN IN CAPITAL LETTERS> --user=<user>
   ```

5. Export the keytab file:

   ```
   ipa-getkeytab -s <domain controller address> -p HTTP/<Administration Server host address>@<DOMAIN WRITTEN IN CAPITAL LETTERS> -k /tmp/h.keytab
   ```

## Generating a keytab file for Microsoft Active Directory

*To generate a keytab file:*

1. Create a user account to be used by IAM to communicate with the domain controller.

2. Enable the following options for the user account:

   - **User cannot change password**
   - **Kerberos AES 256-bit encryption**

   You can enable the **Password never expires** option to avoid reissuing the keytab file each time the password expires.

3. Add a Service Principal Name (SPN) to the user account:

   ```
   setspn -S HTTP/<Administration Server host FQDN> <DOMAIN WRITTEN IN CAPITAL LETTERS>\<user>
   ```

4. Export the keytab file:

   ```
   ktpass -out C:\<folder>\<keytab file name> -princ HTTP/<Administration Server host FQDN>@<DOMAIN WRITTEN IN CAPITAL LETTERS> -mapuser <DOMAIN WRITTEN IN CAPITAL LETTERS>\<user> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <password> -mapop set
   ```

## Generating a keytab file for Samba

*To generate a keytab file:*

1. Create a user account to be used by IAM to communicate with the domain controller:

   ```
   samba-tool user add <user>
   ```

2. Add the SPN to the user account:

   ```
   samba-tool spn add HTTP/<Administration Server host FQDN> <user>
   ```

3. Export the keytab file:

   ```
   samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/<Administration Server host FQDN>
   ```

## Enabling Kerberos domain authentication

*To enable Kerberos domain authentication:*

1. Perform domain controller polling.
2. In the main menu, go to the **Settings** → **Single sign-on** section.
3. Enable the **Kerberos authentication** option.
4. Upload the keytab file.
5. Assign a role to domain users that gives access to Kaspersky Security Center Web Console.

   Kerberos domain authentication is enabled for domain users.

# Updating Kaspersky databases and applications

This section describes steps you must take to regularly update the following:

- Kaspersky databases and software modules
- Installed Kaspersky applications, including Kaspersky Security Center Linux components and security applications

Updates functionality (including providing anti-virus signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

# Scenario: Regular updating Kaspersky databases and applications

This section provides a scenario for regular updating of Kaspersky databases, software modules, and applications. After you complete the Configuring network protection scenario, you must maintain the reliability of the protection system to make sure that the Administration Servers and managed devices are kept protected against various threats, including viruses, network attacks, and phishing attacks.

Network protection is kept up-to-date by regular updates of the following:

- Kaspersky databases and software modules
- Installed Kaspersky applications, including Kaspersky Security Center Linux components and security applications

When you complete this scenario, you can be sure of the following:

- Your network is protected by the most recent Kaspersky software, including Kaspersky Security Center Linux components and security applications.
- The anti-virus databases and other Kaspersky databases critical for the network safety are always up-to-date.

## Prerequisites

The managed devices must have a connection to the Administration Server. If they do not have a connection, consider updating Kaspersky databases and software modules manually or directly from the Kaspersky update servers.

Administration Server must have a connection to the internet.

Before you start, make sure that you have done the following:

1. Deployed the Kaspersky security applications to the managed devices according to the scenario of deploying Kaspersky applications through Kaspersky Security Center Web Console.
2. Created and configured all required policies, policy profiles, and tasks according to the scenario of configuring network protection.
3. Assigned an appropriate amount of distribution points in accordance with the number of managed devices and the network topology.

Updating Kaspersky databases and applications proceeds in stages:

**1 Choosing an update scheme**

There are several schemes that you can use to install updates for security applications. Choose the scheme or several schemes that meet the requirements of your network best.

**2 Creating the task for downloading updates to the repository of the Administration Server**

This task is created automatically by Kaspersky Security Center quick start wizard. If you did not run the wizard, create the task now.

This task is required to download updates from Kaspersky update servers to the repository of the Administration Server, as well as to update Kaspersky databases and software modules for Kaspersky Security Center Linux. After the updates are downloaded, they can be propagated to the managed devices.

If your network has assigned distribution points, the updates are automatically downloaded from the Administration Server repository to the repositories of the distribution points. In this case the managed devices included in the scope of a distribution point download the updates from the repository of the distribution point instead of the Administration Server repository.

How-to instructions: Creating the task for downloading updates to the repository of the Administration Server

**3 Creating the task for downloading updates to the repositories of distribution points (optional)**

By default, the updates are downloaded to the distribution points from the Administration server. You can configure Kaspersky Security Center Linux to download the updates to the distribution points directly from Kaspersky update servers. Download to the repositories of distribution points is preferable if the traffic between the Administration Server and the distribution points is more expensive than the traffic between the distribution points and Kaspersky update servers, or if your Administration Server does not have internet access.

When your network has assigned distribution points and the *Download updates to the repositories of distribution points* task is created, the distribution points download updates from Kaspersky update servers, and not from the Administration Server repository.

How-to instructions: Creating the task for downloading updates to the repositories of distribution points

**4 Configuring distribution points**

When your network has assigned distribution points, make sure that the **Enabled** option is enabled in the properties of all required distribution points. When this option is disabled for a distribution point, the devices included in the scope of the distribution point download updates from the repository of the Administration Server.

5. **Optimizing the update process by using the diff files (optional)**

   You can optimize traffic between the Administration Server and the managed devices by using diff files. When this feature is enabled, the Administration Server or a distribution point downloads diff files instead of entire files of Kaspersky databases or software modules. A diff file describes the differences between two versions of a file of a database or software module. Therefore, a diff file occupies less space than an entire file. This results in decrease in the traffic between the Administration Server or distribution points and the managed devices. To use this feature, enable the **Download diff files** option in the properties of the *Download updates to the Administration Server repository* task and/or the *Download updates to the repositories of distribution points* task.

   How-to instructions: Using diff files for updating Kaspersky databases and software modules

6. **Configuring automatic installation of updates for the security applications**

   Create the *Update* tasks for the managed applications to provide timely updates to the software modules and Kaspersky databases, including anti-virus databases. To ensure timely updates, we recommend that you select the **When new updates are downloaded to the repository** option when configuring the task schedule.

   If an update requires reviewing and accepting the terms of the End User License Agreement, then you first need to accept the terms. After that the update can be propagated to the managed devices.

7. **Approving and declining updates of managed Kaspersky applications**

   By default, the downloaded software updates have the *Undefined* status. You can change the status to *Approved* or *Declined*. The approved updates are always installed. If an update of a managed Kaspersky application requires reviewing and accepting the terms of the End User License Agreement, then you first need to accept the terms. After that the update can be propagated to the managed devices. The updates for which you set *Declined* status will not be installed on devices. If a declined update for a managed application was previously installed, Kaspersky Security Center Linux will try to uninstall the update from all devices.

   Approving and declining updates is available only for Network Agent and managed Kaspersky applications installed on the Windows-based and Linux-based client devices. Seamless updating of Administration Server, Kaspersky Security Center Web Console, and management web plug-ins is not supported.

   How-to instructions: Approving and declining software updates

   Sometimes after Network Agent update you may be prompted to restart managed devices. If the notification about the required restart is displayed, click the **View devices** link in the notification, select the check boxes next to the devices to be restarted, and then click the **Restart** button to finish the Network Agent update.

## Results

Upon completion of the scenario, Kaspersky Security Center Linux is configured to update Kaspersky databases after the updates are downloaded to the repository of the Administration Server. You can then proceed to monitoring the network status.

# About updating Kaspersky databases, software modules, and applications

To be sure that the protection of your Administration Servers and managed devices is up-to-date, you must provide timely updates of the following:

- Kaspersky databases and software modules

  Before downloading Kaspersky databases and software modules, Kaspersky Security Center Linux checks if Kaspersky servers are accessible. If access to the servers using system DNS is not possible, the application uses public DNS servers. This is necessary to make sure anti-virus databases are updated and the level of security is maintained for the managed devices.

- Installed Kaspersky applications, including Kaspersky Security Center Linux components and security applications

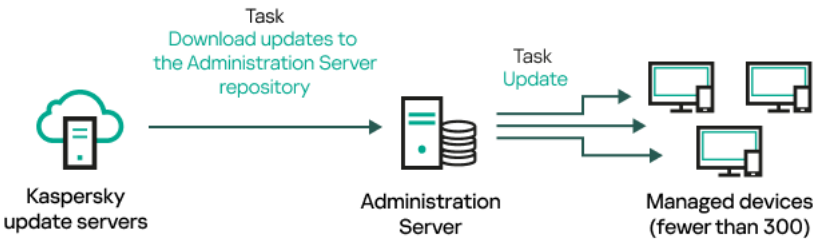
  Kaspersky Security Center Linux allows you to update Network Agent and Kaspersky applications installed on Windows-based and Linux-based client devices automatically. Seamless updating of Administration Server, Kaspersky Security Center Web Console, and management web plug-ins is not supported. To update these components, you have to download the latest versions from the Kaspersky website, and then install them manually.

Depending on the configuration of your network, you can use the following schemes of downloading and distributing the required updates to the managed devices:

- By using a single task: *Download updates to the Administration Server repository*
- By using two tasks:
  - The *Download updates to the Administration Server repository* task
  - The *Download updates to the repositories of distribution points* task
- Manually through a shared folder or an FTP server
- Directly from Kaspersky update servers to Kaspersky Endpoint Security on the managed devices
- Through a local or network folder if Administration Server has no internet connection

## Using the Download updates to the Administration Server repository task

In this scheme, Kaspersky Security Center Linux downloads updates through the *Download updates to the Administration Server repository* task. In small networks that contain less than 300 managed devices in a single network segment or less than 10 managed devices in each network segment, the updates are distributed to the managed devices directly from the Administration Server repository (see figure below).



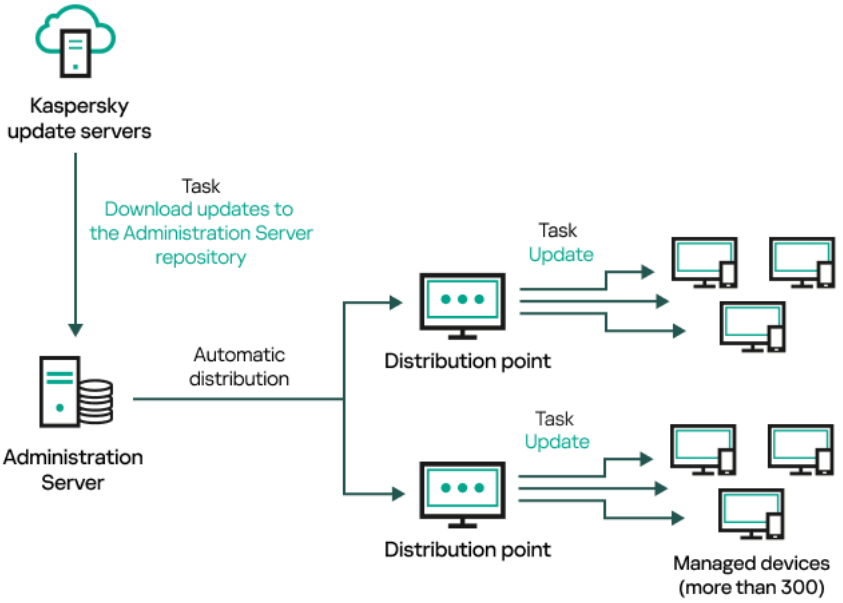

Updating by using the *Download updates to the Administration Server repository* task without distribution points

As a source of updates, you can use not only Kaspersky update servers, but also a local or network folder.

By default, the Administration Server communicates with Kaspersky update servers and downloads updates by using the HTTPS protocol. You can configure the Administration Server to use the HTTP protocol instead of HTTPS.

If your network contains 300 managed devices or more in a single network segment or if your network consists of several network segments with more than 9 managed devices in each network segment, we recommend that you use distribution points to propagate the updates to the managed devices (see figure below). Distribution points reduce the load on the Administration Server and optimize traffic between the Administration Server and the managed devices. You can calculate the number and configuration of distribution points required for your network.

In this scheme, the updates are automatically downloaded from the Administration Server repository to the repositories of the distribution points. The managed devices included in the scope of a distribution point download the updates from the repository of the distribution point instead of the Administration Server repository.




Updating by using the *Download updates to the Administration Server repository* task with distribution points

When the *Download updates to the Administration Server repository* task is complete, the updates for Kaspersky databases and software modules for Kaspersky Endpoint Security are downloaded to the Administration Server repository. These updates are installed through the *Update* task for Kaspersky Endpoint Security.

The *Download updates to the repository of the Administration Server* task is not available on virtual Administration Servers. The repository of the virtual Administration Server displays updates downloaded to the primary Administration Server.

You can configure the updates to be verified for operability and errors on a set of test devices. If the verification is successful, the updates are distributed to other managed devices.

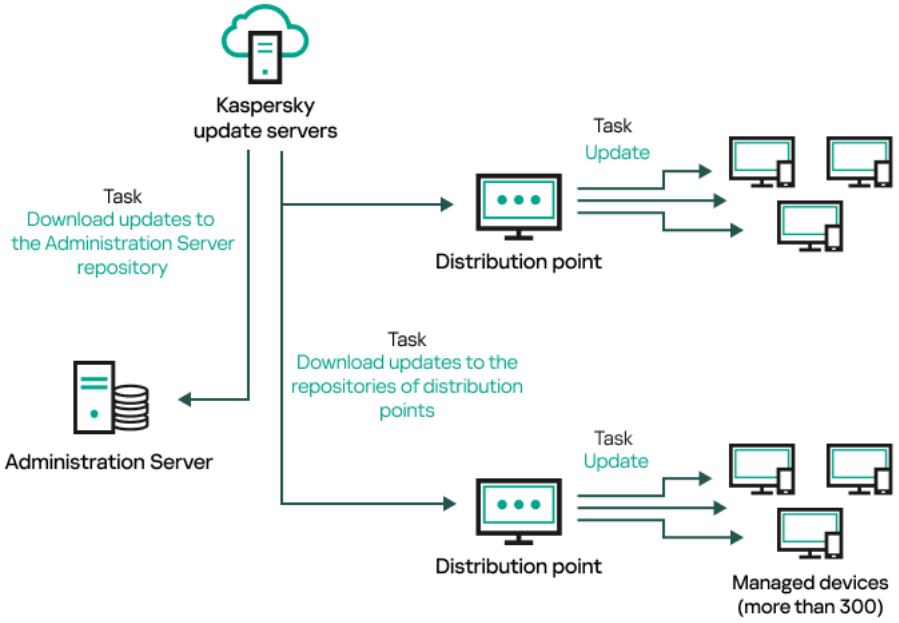
Each Kaspersky application requests required updates from Administration Server. Administration Server aggregates these requests and downloads only those updates that are requested by any application. This ensures that the same updates are not downloaded multiple times and that unnecessary updates are not downloaded at all. When running the *Download updates to the Administration Server repository* task, Administration Server sends the following information to Kaspersky update servers automatically in order to ensure the downloading of relevant versions of Kaspersky databases and software modules:

- Application ID and version
- Application setup ID
- Active key ID
- *Download updates to the repository of the Administration Server* task run ID

None of the transmitted information contains personal or other confidential data. AO Kaspersky Lab protects information in accordance with requirements established by law.

## Using two tasks: the Download updates to the Administration Server repository task and the Download updates to the repositories of distribution points task

You can download updates to the repositories of distribution points directly from the Kaspersky update servers instead of the Administration Server repository, and then distribute the updates to the managed devices (see figure below). Download to the repositories of distribution points is preferable if the traffic between the Administration Server and the distribution points is more expensive than the traffic between the distribution points and Kaspersky update servers, or if your Administration Server does not have internet access.




Updating by using the *Download updates to the Administration Server repository* task and the *Download updates to the repositories of distribution points task*

By default, the Administration Server and distribution points communicate with Kaspersky update servers and

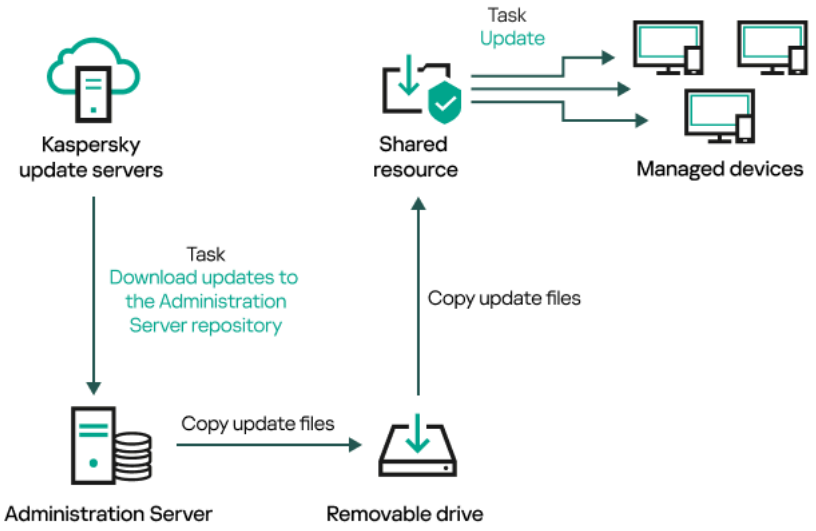
download updates by using the HTTPS protocol. You can configure the Administration Server and/or distribution points to use the HTTP protocol instead of HTTPS.

To implement this scheme, create the *Download updates to the repositories of distribution points* task in addition to the *Download updates to the Administration Server repository* task. After that the distribution points will download updates from Kaspersky update servers, and not from the Administration Server repository.

The *Download updates to the Administration Server repository* task is also required for this scheme, because this task is used to download Kaspersky databases and software modules for Kaspersky Security Center Linux.

### Manually through a shared folder or an FTP server

If the client devices do not have a connection to the Administration Server, you can use a local folder or a shared resource as a source for updating Kaspersky databases, software modules, and applications. In this scheme, you need to copy required updates from the Administration Server repository to a removable drive, then copy the updates to the local folder or the shared resource specified as an update source in the settings of Kaspersky Endpoint Security (see figure below).



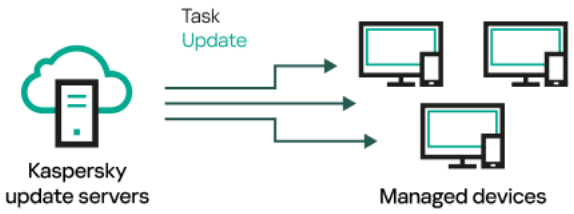

Updating through a local folder, a shared folder, or an FTP server

For more information about sources of updates in Kaspersky Endpoint Security, see the following Helps:

- Kaspersky Endpoint Security for Linux Help
- Kaspersky Endpoint Security for Windows Help

### Directly from Kaspersky update servers to Kaspersky Endpoint Security on the managed devices

On the managed devices, you can configure Kaspersky Endpoint Security to receive updates directly from Kaspersky update servers (see figure below).




Updating security applications directly from Kaspersky update servers

In this scheme, the security application does not use the repository provided by Kaspersky Security Center Linux. To receive updates directly from Kaspersky update servers, specify Kaspersky update servers as an update source in the security application. For more information about these settings, see the following Helps:

- Kaspersky Endpoint Security for Linux Help
- Kaspersky Endpoint Security for Windows Help

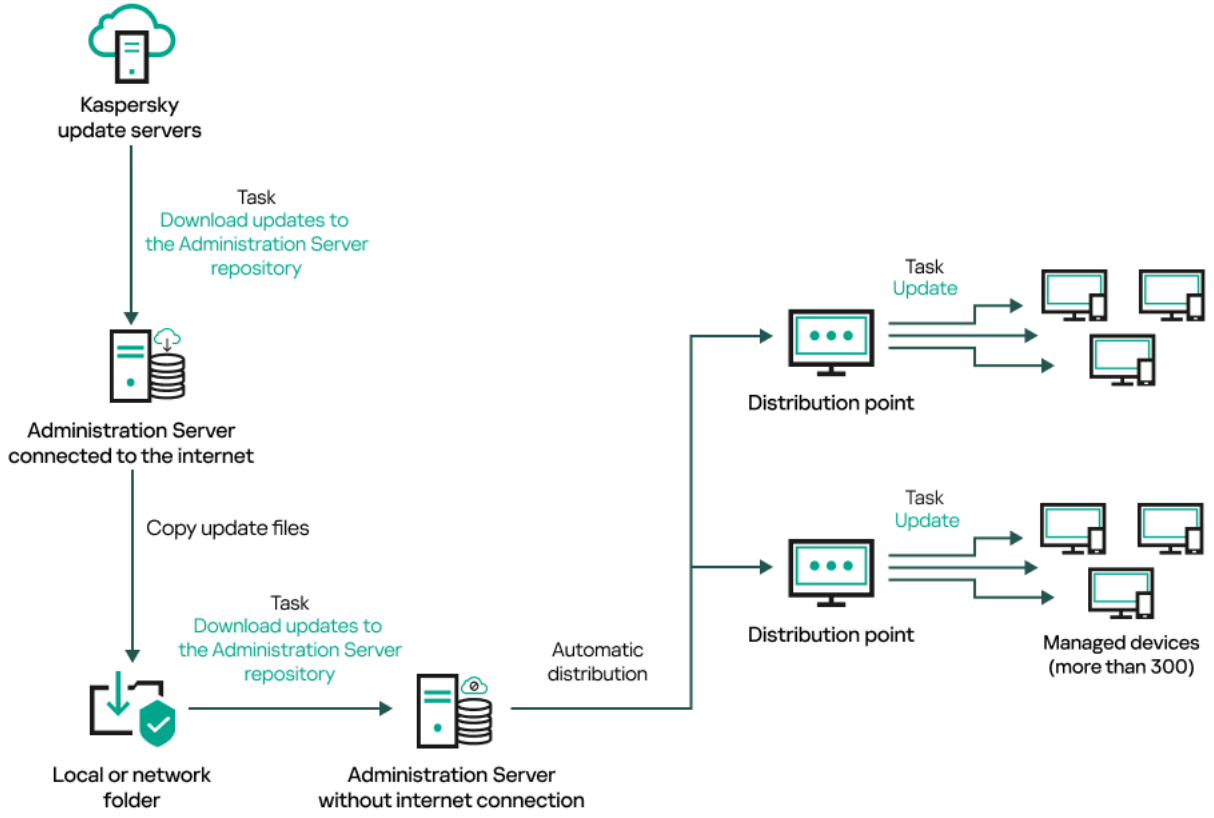
### Through a local or network folder if Administration Server has no internet connection

If Administration Server has no internet connection, you can configure the *Download updates to the Administration Server repository* task to download updates from a local or network folder. In this case, you must copy the required update files to the specified folder from time to time. For example, you can copy the required update files from one of the following sources:

- Administration Server that has an internet connection (see the figure below)

  Because an Administration Server downloads only the updates that are requested by the security applications, the sets of security applications managed by the Administration Servers—the one that has an internet connection and the one that does not—must match.

If the Administration Server that you use to download updates has version 13.2 or earlier, open properties of the *Download updates to the Administration Server repository* task, and then enable the **Download updates by using the old scheme** option.




Updating through a network folder if Administration Server has no internet connection

- Kaspersky Update Utility

  Because this utility uses the old scheme to download updates, open properties of the *Download updates to the Administration Server repository* task, and then enable the *Download updates by using the old scheme* option. If necessary, you can also configure the *Download the update request file automatically* option so that the Kaspersky Update Utility downloads only the required updates.

# Creating the Download updates to the Administration Server repository task

The *Download updates to the Administration Server repository* task allows you to download updates of databases and software modules for Kaspersky security applications from Kaspersky update servers to the Administration Server repository.

The *Download updates to the Administration Server repository* task is created automatically when the Administration Server is started. In the list of tasks, there can only be one *Download updates to the Administration Server repository* task. You can create this task again if it is removed from the task list of the Administration Server.

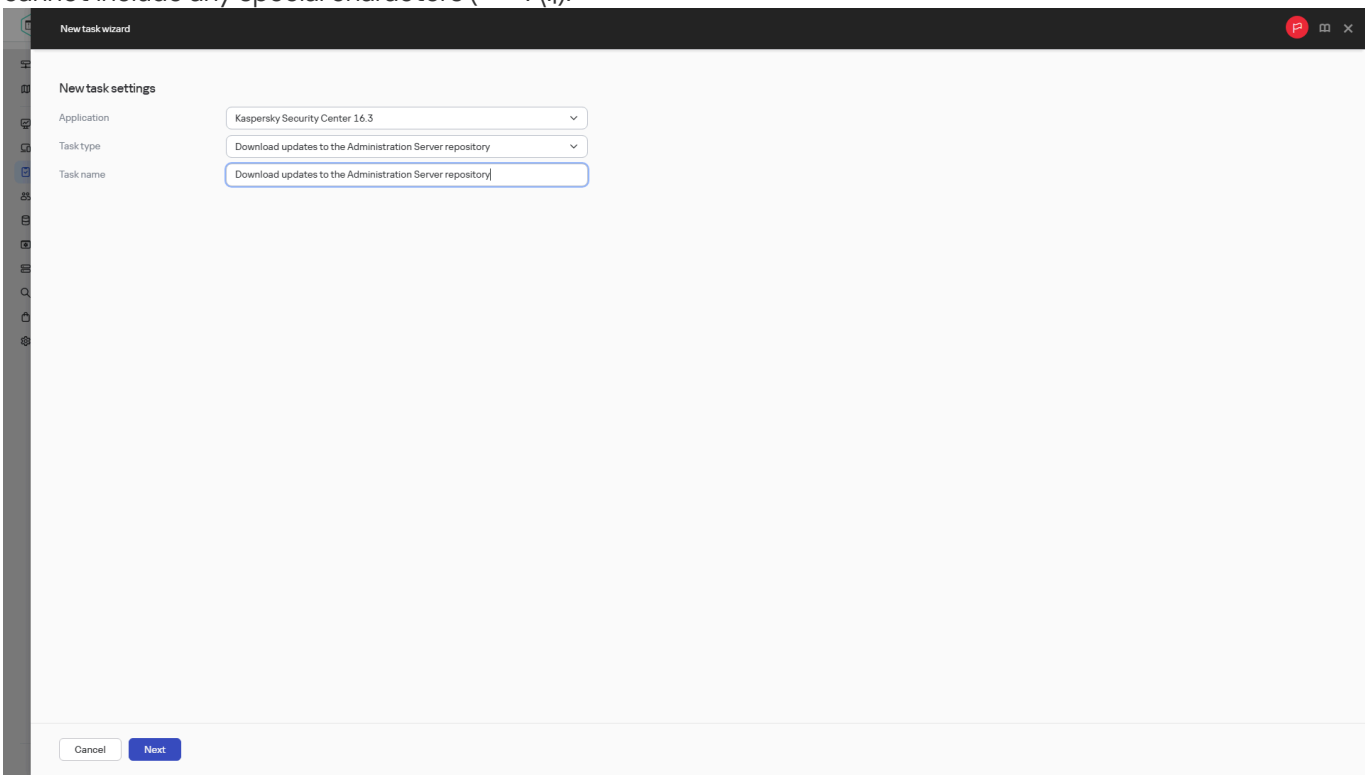
After the *Download updates to the Administration Server repository* task is complete and the updates are downloaded, they can be propagated to the managed devices.

Before you distribute updates to the managed devices, you can run the *Update verification* task. This allows you to make sure that Administration Server installs the downloaded updates properly and a security level is not decreased because of the updates. To verify them before distributing, configure the **Run update verification** option in the *Download updates to the Administration Server repository* task settings.

*To create a Download updates to the Administration Server repository task:*

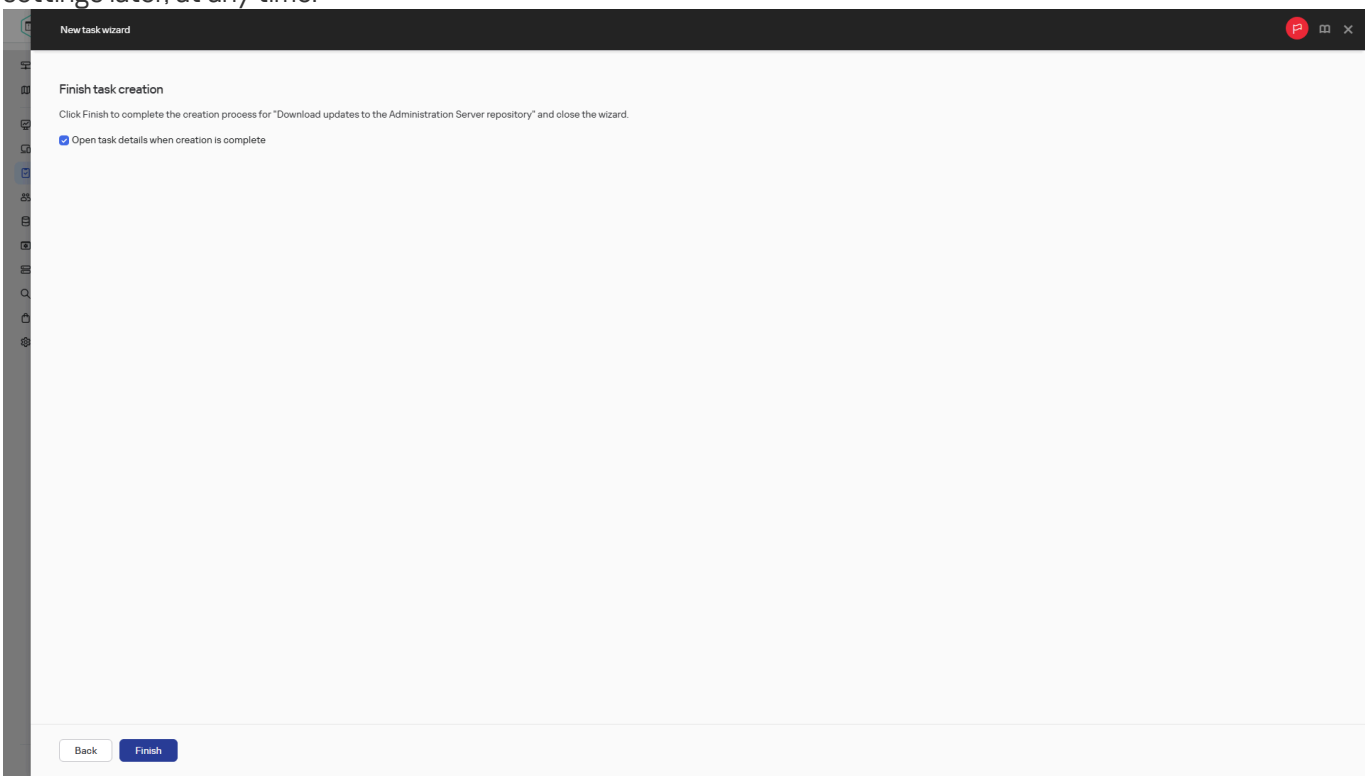
1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts. Follow the steps of the wizard.
3. For the Kaspersky Security Center application, select the **Download updates to the Administration Server repository** task type.
4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).




Creating the Download updates to the Administration Server repository task

5. On the **Finish task creation** page, you can enable the **Open task details when creation is complete** option to open the task properties window and modify the default task settings. Otherwise, you can configure the task settings later, at any time.




Finishing task creation

6. Click the **Finish** button.

   The task is created and displayed in the list of tasks.

7. Click the created task name to open the task properties window.

8. In the task properties window, on the **Application settings** tab, specify the following settings:

   **Sources of updates**

   As a source of updates, you can use:

   - Kaspersky update servers (selected by default)
   - Primary Administration Server

     This resource applies to tasks created for a secondary or virtual Administration Server.
   - Local or network folder

     A local or network folder that contains the latest updates. A network folder can be an FTP or HTTP server, or an SMB share.

     When selecting a local folder, you must specify a folder on the device that has Administration Server installed. The path to the folder depends on the device's operating system. Since the local folder is located on Linux-based Administration Server, you have to specify the POSIX path, for example: /path/to/dir.

     When selecting an SMB network folder as an update source, mount the folder on the device where the Administration Server is installed before selecting it. Then specify the path to the mounted folder by using its local file system path. Access to the folder is performed by using the SMB protocol.

A local or network folder or an FTP or HTTP server used as an update source must contain a folder structure that matches the folder structure on the Kaspersky update servers. You can obtain this structure by using Kaspersky Update Utility.

In the *Download updates to the Administration Server repository* task and the *Download updates to the repositories of distribution points* task, user authentication does not work if you select a password-protected local or network folder as an update source. To resolve this issue, first mount the password-protected folder, and then specify the required credentials, for example, by means of the operating system. After that, you can select this folder as an update source in an update download task. Kaspersky Security Center Linux will not require that you enter the credentials.

**Folder for storing updates**

The path to the specified folder for storing saved updates. You can copy the specified folder path to a clipboard. You cannot change the path to a specified folder for a group task.

**Force update of secondary Administration Servers**

If this option is enabled, the Administration Server starts update tasks on the secondary Administration Servers as soon as new updates are downloaded. Update tasks are started by using the source of update that is configured in the task properties on the secondary Administration Servers.

If this option is disabled, the update tasks on the secondary Administration Servers start according to their schedules.

By default, this option is disabled.

**Copy downloaded updates to additional folders**

After the Administration Server receives updates, it copies them to the specified folders. Use this option if you want to manually manage the distribution of updates on your network.

For example, you may want to use this option in the following situation: the network of your organization consists of several independent subnets, and devices from each of the subnets do not have access to other subnets. However devices in all of the subnets have access to a common network share. In this case, you set Administration Server in one of the subnets to download updates from Kaspersky update servers, enable this option, and then specify this network share. In downloaded updates to the repository tasks for other Administration Servers, specify the same network share as the update source.

If you select to copy the downloaded updates to a local folder, you must specify a folder on the device that has Administration Server installed. The path to the folder depends on the device's operating system. Since the local folder is located on Linux-based Administration Server, you have to specify the POSIX path, for example: /path/to/dir.

When selecting a network folder that is located on Linux-based Administration Server, you must ensure access to the network folder in advance from the device with Administration Server installed by mounting the folder. Access to the folder is performed by using the SMB protocol.

By default, this option is disabled.

**Download diff files**

This option enables the downloading diff files feature.

By default, this option is disabled.

**Download updates by using the old scheme**

Starting from version 14, Kaspersky Security Center downloads updates of databases and software modules by using the new scheme. For the application to download updates by using the new scheme, the update source must contain the update files with the metadata compatible with the new scheme. If the update source contains the update files with the metadata compatible with the old scheme only, enable the **Download updates by using the old scheme** option. Otherwise, the update download task will fail.

For example, you must enable this option when a local or network folder is specified as an update source and the update files in this folder were downloaded by one of the following applications:

- Kaspersky Update Utility

  This utility downloads updates by using the old scheme.

- Kaspersky Security Center 13 Linux

  For example, your Administration Server 1 does not have an internet connection. In this case, you may download updates by using an Administration Server 2 that has an internet connection, and then place the updates to a local or network folder to use it as an update source for the Administration Server 1. If the Administration Server 2 has version 13, enable the **Download updates by using the old scheme** option in the task for the Administration Server 1.

By default, this option is disabled.

**Run update verification**

Administration Server downloads updates from the source, saves them to a temporary repository, and runs the task defined in the **Update verification task** field. If the task completes successfully, the updates are copied from the temporary repository to a shared folder on the Administration Server and then distributed to all devices for which the Administration Server acts as the source of updates (tasks with the **When new updates are downloaded to the repository** schedule type are started). The task of downloading updates to the repository is finished only after completion of the *Update verification* task.

By default, this option is disabled.

**Download the update request file automatically**

If you want Kaspersky Update Utility to download only the required updates with suitable configuration, enable this option and specify the path where Kaspersky Security Center Linux will create the update request file with information about the updates to be downloaded. The update request file contains the timestamp and the MD5 hash for version control.

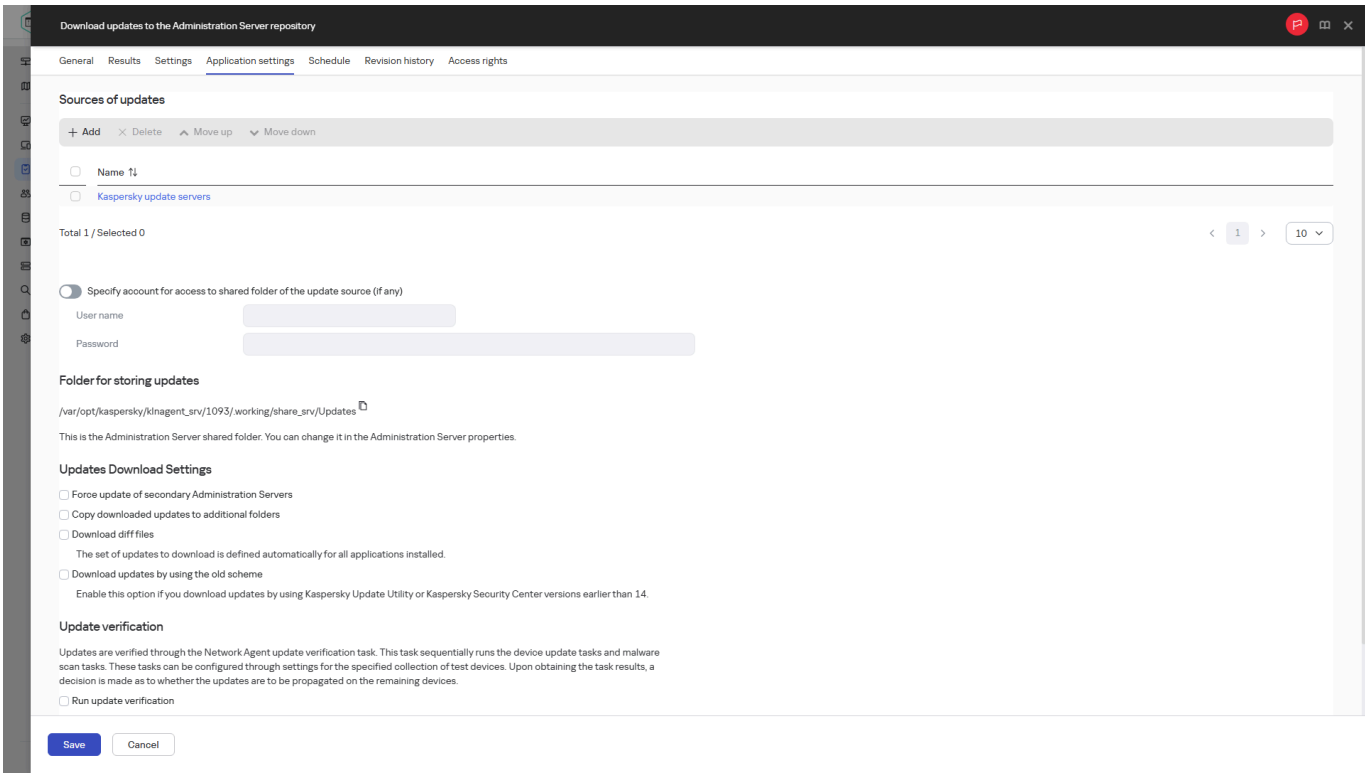
Make sure that the **Download updates by using the old scheme** option is disabled.

Also, the update download in Kaspersky Update Utility must be configured.

By default, the following path is specified: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml. If necessary, you can change the default name (retranslation_request) and path.

> The request file can be placed at a local or shared folder. When using a shared folder, you have to ensure the access to this folder from the device with Administration Server installed. The ways to ensure the access and the tools used depend on your infrastructure.

When performing the *Download updates to the Administration Server repository* task, Kaspersky Security Center Linux creates the update request file in the .xml format at the path that you have specified. Kaspersky Update Utility automatically obtains the information from the request file, and then downloads only the required updates. If Kaspersky Update Utility is unable to obtain the information automatically (for example, Kaspersky Update Utility does not have access to the folder where Kaspersky Security Center Linux created the request file), you have to transmit the file by using third-party tools.




Specifying the properties of the Download updates to the Administration Server repository task

9. In the task properties window, on the **Schedule** tab, create a schedule for task start. If necessary, configure the following settings:

- **Start task**:

  **Manually** (selected by default)

  The task does not run automatically. You can only start it manually.

  By default, this option is selected.

  **Every N minutes**

  The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

  By default, the task runs every 30 minutes, starting from the current system time.

  **Every N hours**

  The task runs regularly, with the specified interval in hours, starting from the specified date and time.

  By default, the task runs every 6 hours, starting from the current system date and time.

  **Every N days**

  The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

  By default, the task runs every day, starting from the current system date and time.

**By days of week**

The task runs regularly, on the specified days of the week, at the specified time.

By default, the task runs every Friday at 6:00:00 PM.

**Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

**Monthly on selected weekday**

The task runs regularly, on the specified days of each month, at the specified time.

By default, the start time is 18:00, and no days of the month are selected.

> Note that you select neither a specific date in the month, nor the number of the week (first, second week of the month) but the sequence number of the weekday within a month. For example, if you set the cursor in the **Tu** cell of the **First** row, it means the task will run every first Tuesday of each new month.

You can select several days of week.

**On completing another task**

The current task starts after another task completes. This option only works if both tasks are assigned to the same devices. For example, you may want to run the *Manage devices* task with the **Turn on the device** option and, after it completes, run the *Virus scan* task as a triggering task.

You have to select the triggering task from the table and the status with which this task must complete (**Completed successfully** or **Failed**).

If necessary, you can search, sort, and filter the tasks in the table as follows:

- Enter the task name in the search field, to search the task by its name.
- Click the sort icon to sort the tasks by name.

  By default, the tasks are sorted in alphabetical ascending order.
- Click the filter icon, and in the window that opens, filter the tasks by group, and then click the **Apply** button.

- Additional task settings:

  **Run missed tasks**

  This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

  If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

  If this option is disabled, only scheduled tasks run on client devices. For **Manually**, **Once** and **Immediately** schedule, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

**Use automatically randomized delay for task starts**

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However, when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is enabled.

**Use automatically randomized delay for task starts within an interval of**

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

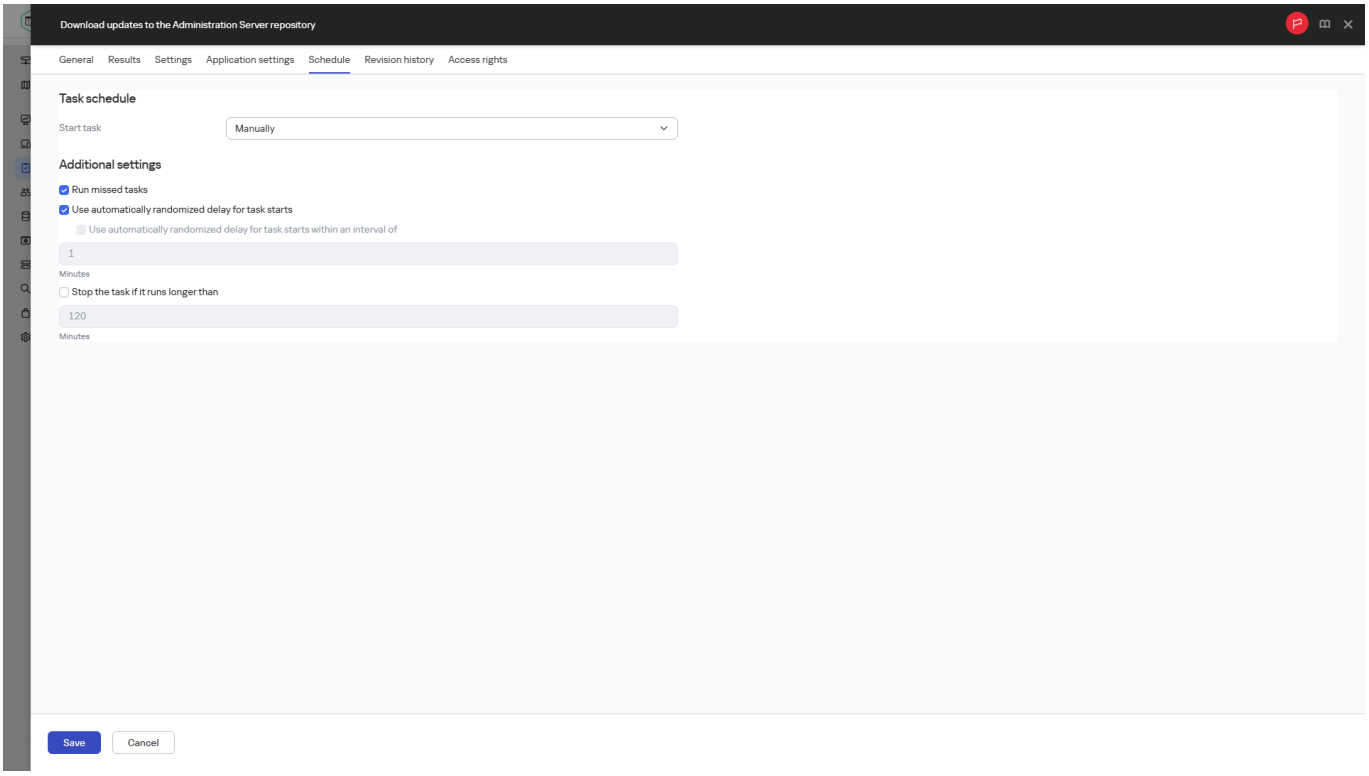
By default, this option is disabled. The default time interval is one minute.

**Stop the task if it runs longer than**

After the specified time period expires, the task is stopped automatically, whether it is completed or not.

Enable this option if you want to interrupt (or stop) tasks that take too long to execute.

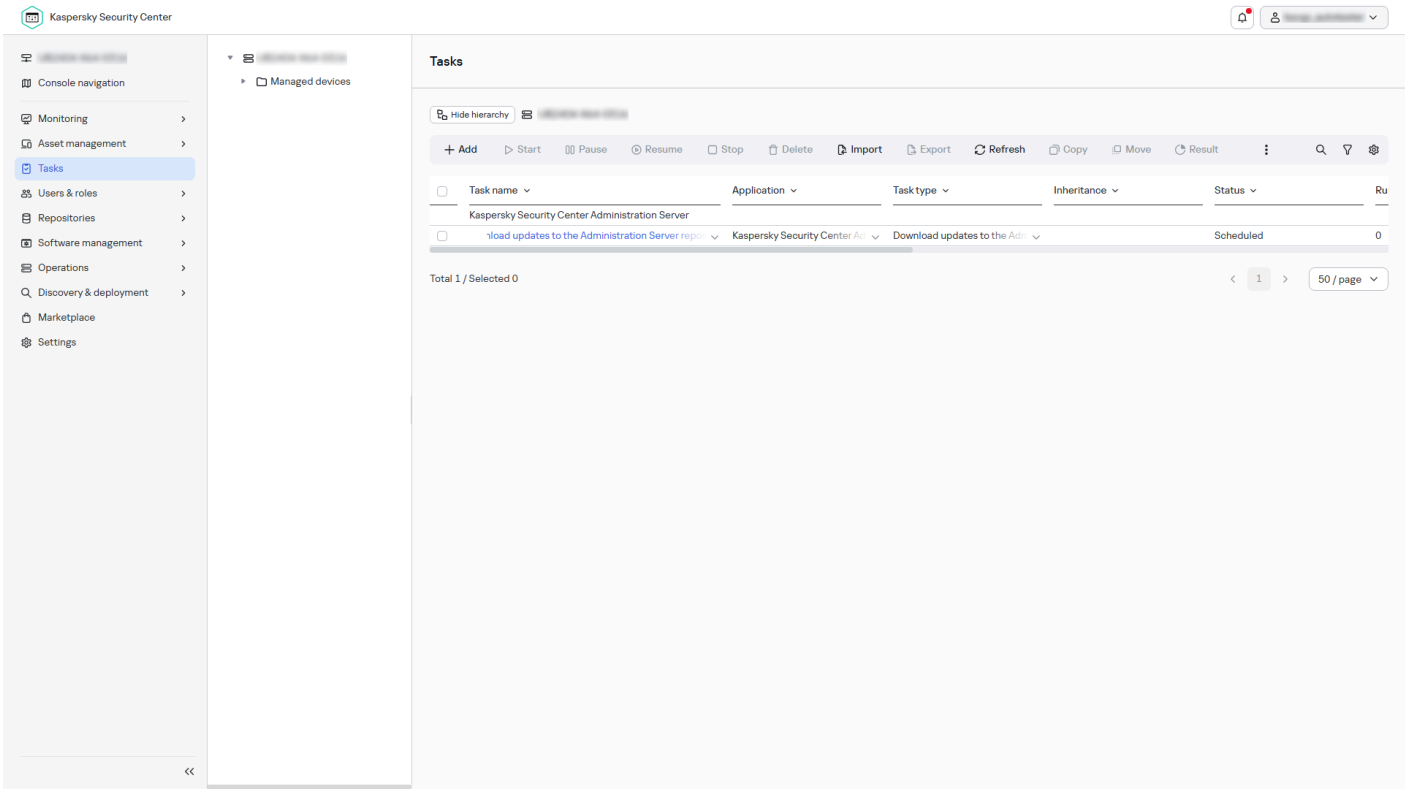
By default, this option is disabled. The default task execution time is 120 minutes.




Specifying the schedule of the Download updates to the Administration Server repository task

10. Click the **Save** button.

The task is created and configured.




The task list

When Administration Server performs the *Download updates to the Administration Server repository* task, updates to databases and software modules are downloaded from the updates source and stored in the shared folder of Administration Server. If you create this task for an administration group, it will only be applied to Network Agents included in the specified administration group.

Updates are distributed to client devices and secondary Administration Servers from the shared folder of Administration Server.

# Verifying downloaded updates

Before installing updates to the managed devices, you can first check the updates for operability and errors through the *Update verification* task. The *Update verification* task is performed automatically as part of the *Download updates to the Administration Server repository* task. The Administration Server downloads updates from the source, saves them in the temporary repository, and runs the *Update verification* task. If the task completes successfully, the updates are copied from the temporary repository to the Administration Server shared folder. They are distributed to all client devices for which the Administration Server is the source of updates.

If, as a result of the *Update verification* task, updates located in the temporary repository are incorrect or if the Update verification task completes with an error, such updates are not copied to the shared folder. The Administration Server retains the previous set of updates. Also, the tasks that have the **When new updates are downloaded to the repository** schedule type are not started then. These operations are performed at the next start of the *Download updates to the Administration Server repository* task if scanning of the new updates completes successfully.

A set of updates is considered invalid if any of the following conditions is met on at least one test device:

- An update task error occurred.
- The real-time protection status of the security application changed after the updates were applied.

- An infected object was detected during running of the on-demand scan task.
- A runtime error of a Kaspersky application occurred.

If none of the listed conditions is true for any test device, the set of updates is considered valid, and the *Update verification* task is considered to have completed successfully.

Before you start to create the *Update verification* task, perform the prerequisites:

1. Create an administration group with several test devices. You will need this group to verify the updates.

   We recommend using devices with the most reliable protection and the most popular application configuration across the network. This approach increases the quality and probability of virus detection during scans, and minimizes the risk of false positives. If viruses are detected on test devices, the *Update verification* task is considered unsuccessful.

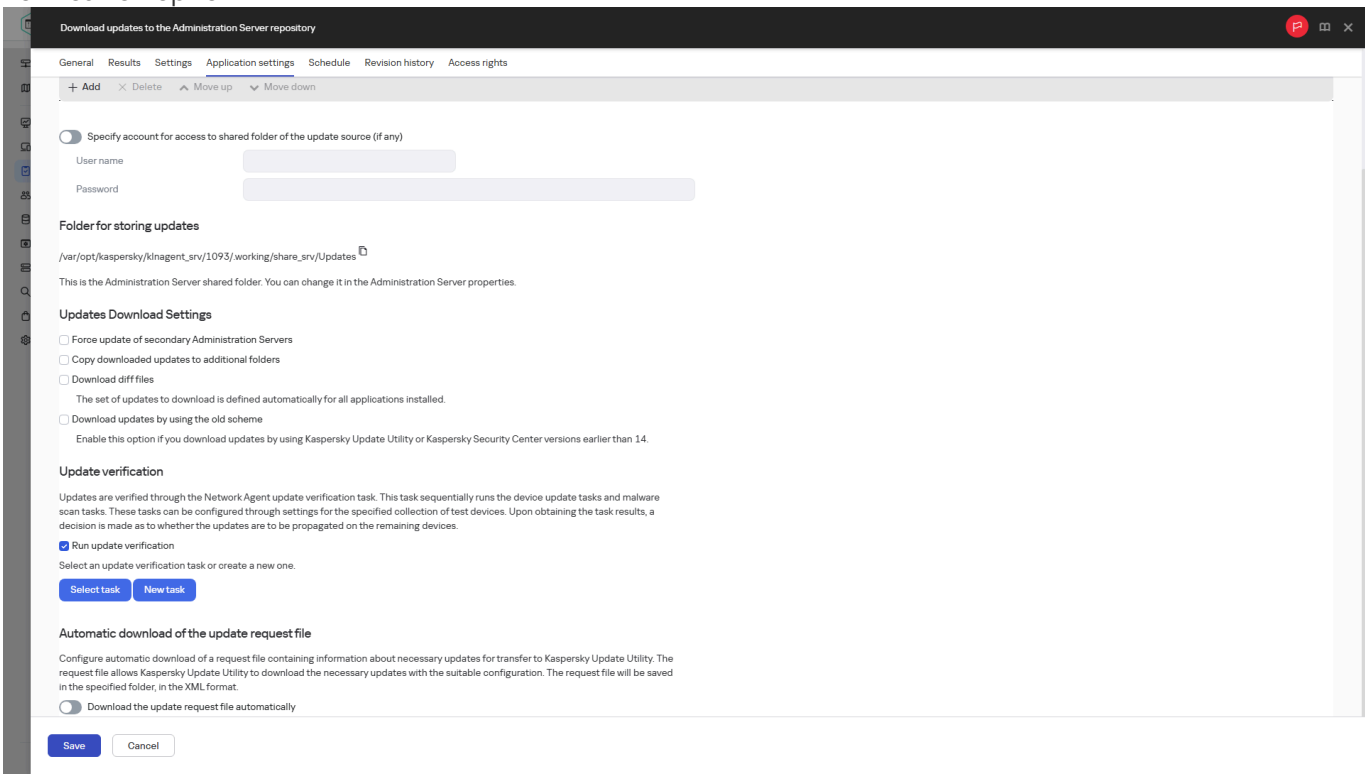
2. Create the update and malware scan tasks for an application supported by Kaspersky Security Center Linux, for example, Kaspersky Endpoint Security for Linux. When creating the update and malware scan tasks, specify the administration group with the test devices.

   The *Update verification* task sequentially runs the update and malware scan tasks on test devices to check that all updates are valid. In addition, when creating the *Update verification* task, you need to specify the update and malware scan tasks.

3. Create the *Download updates to the Administration Server repository* task.

*To make Kaspersky Security Center Linux verify downloaded updates before distributing them to client devices:*

1. In the main menu, go to **Tasks**.
2. Click the **Download updates to the Administration Server repository** task.
3. In the task properties window that opens, go to the **Application settings** tab, and then enable the **Run update verification** option.



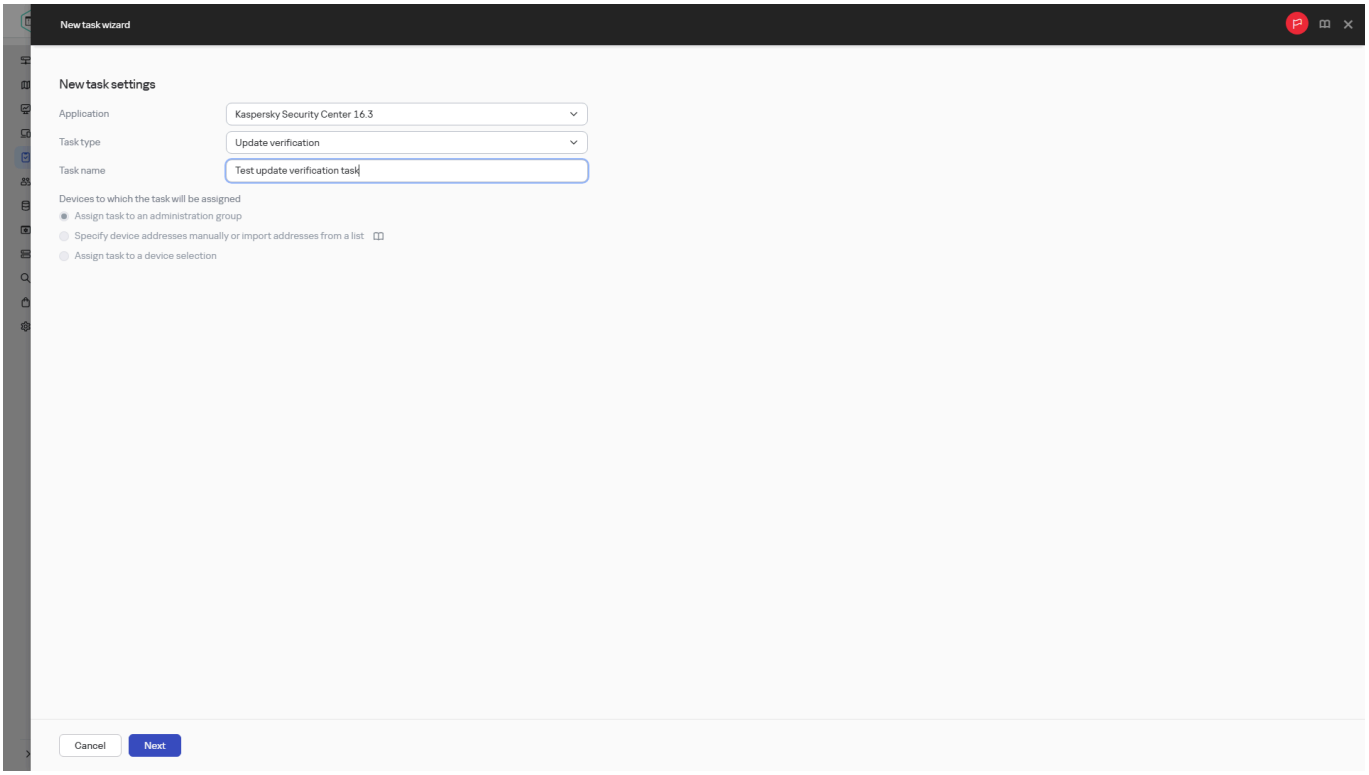

Properties of the Download updates to the Administration Server repository task

4. If the *Update verification* task exists, click the **Select task** button. In the window that opens, select the *Update verification* task in the administration group with test devices.

5. If you did not create the *Update verification* task earlier, do the following:

a. Click the **New task** button.

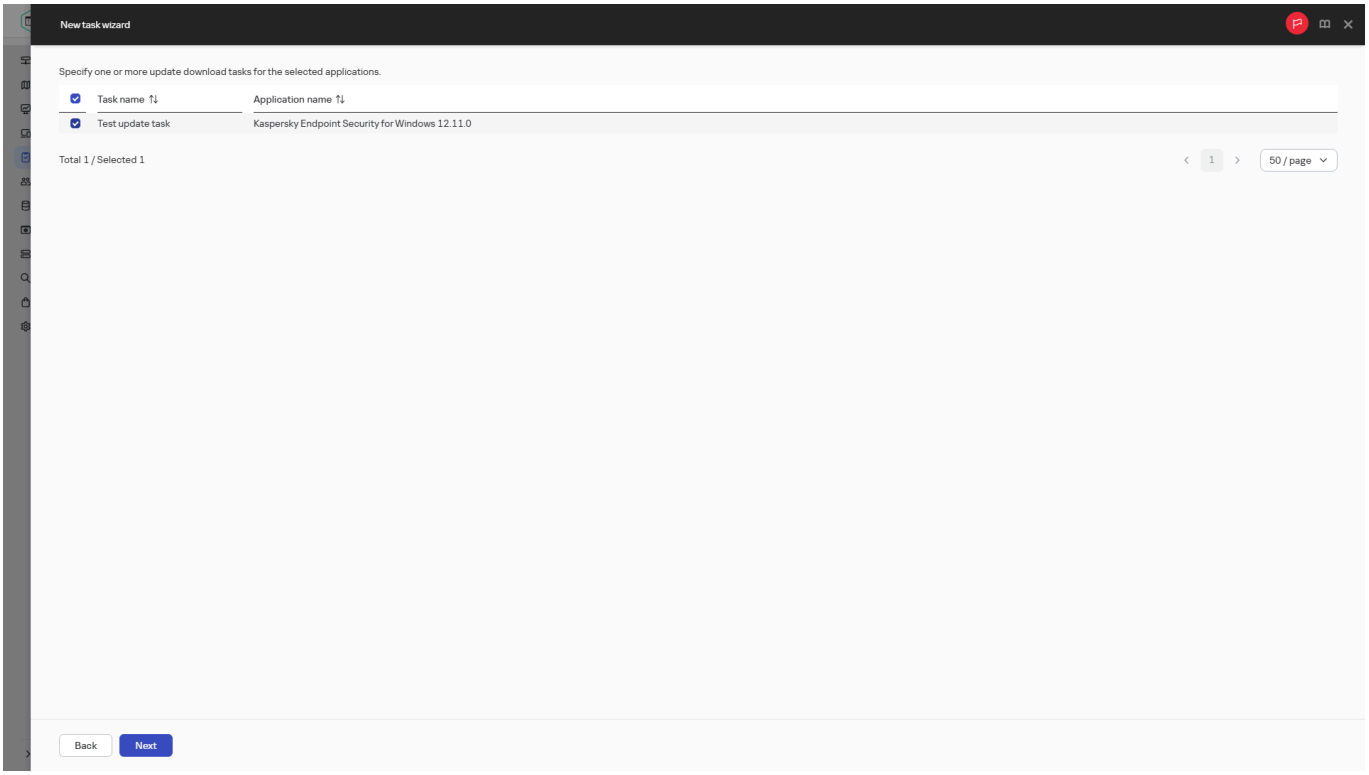
b. In the New task wizard that opens, specify the task name if you want to change the preset name.




Creating an Update verification task

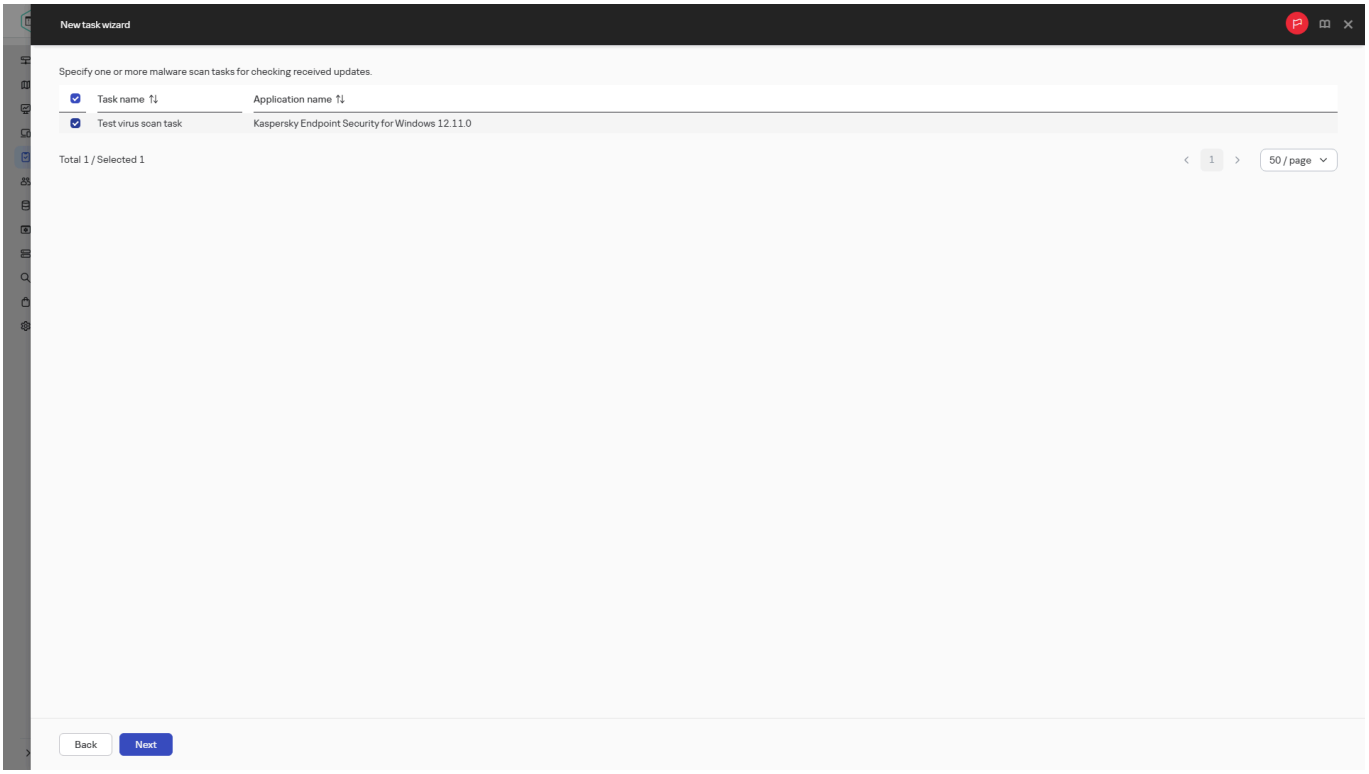
a. Select the administration group with test devices, which you created earlier.

b. Select the update task of a required application supported by Kaspersky Security Center Linux.




Selecting the application update task

a. Select the malware scan task of a required application supported by Kaspersky Security Center Linux.




Selecting the malware scan task

After that, the following options appear. We recommend leaving them enabled:

**Restart the device after database update**

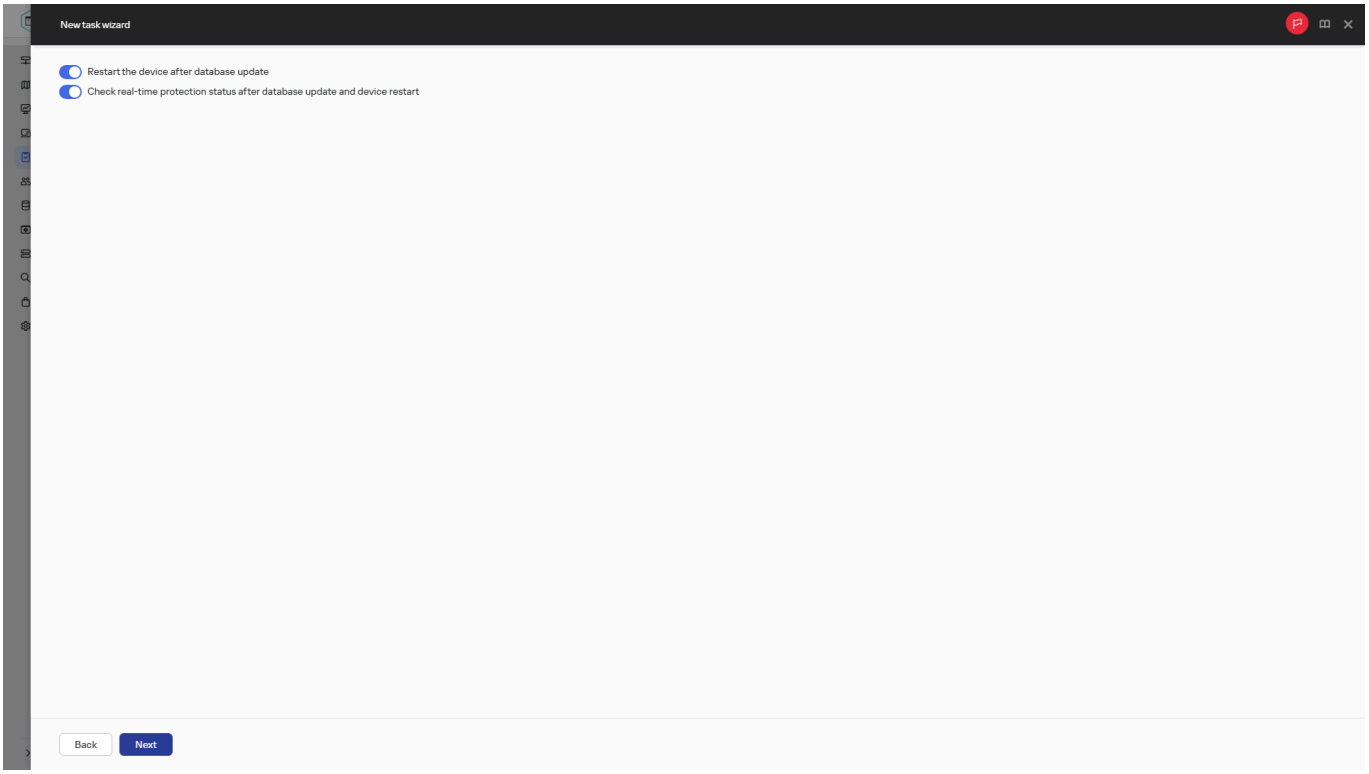
After anti-virus databases are updated on a device, we recommend rebooting the device.

By default, this option is enabled.

**Check real-time protection status after database update and device restart**

If this option is enabled, the *Update verification* task checks whether updates downloaded to the Administration Server repository are valid, and if the protection level decreased after the anti-virus database update and device restart.

By default, this option is enabled.




Specifying the task settings

a. Specify an account from which the *Update verification* task will be run. You can use your account and keep the **Default account** option enabled. Alternatively, you can specify that the task should be run under another account that has the necessary access rights. To do this, select the **Specify account** option, and then enter the credentials of that account.

6. Click **Save** to close the properties window of the *Download updates to the Administration Server repository* task.

The automatic update verification is enabled. Now, you can run the *Download updates to the Administration Server repository* task, and it will start from update verification.

# Creating the task for downloading updates to the repositories of distribution points

You can create the *Download updates to the repositories of distribution points* task for an administration group. This task will run for distribution points included in the specified administration group.

You can use this task, for example, if traffic between the Administration Server and the distribution point(s) is more expensive than traffic between the distribution point(s) and Kaspersky update servers, or if your Administration Server does not have internet access.

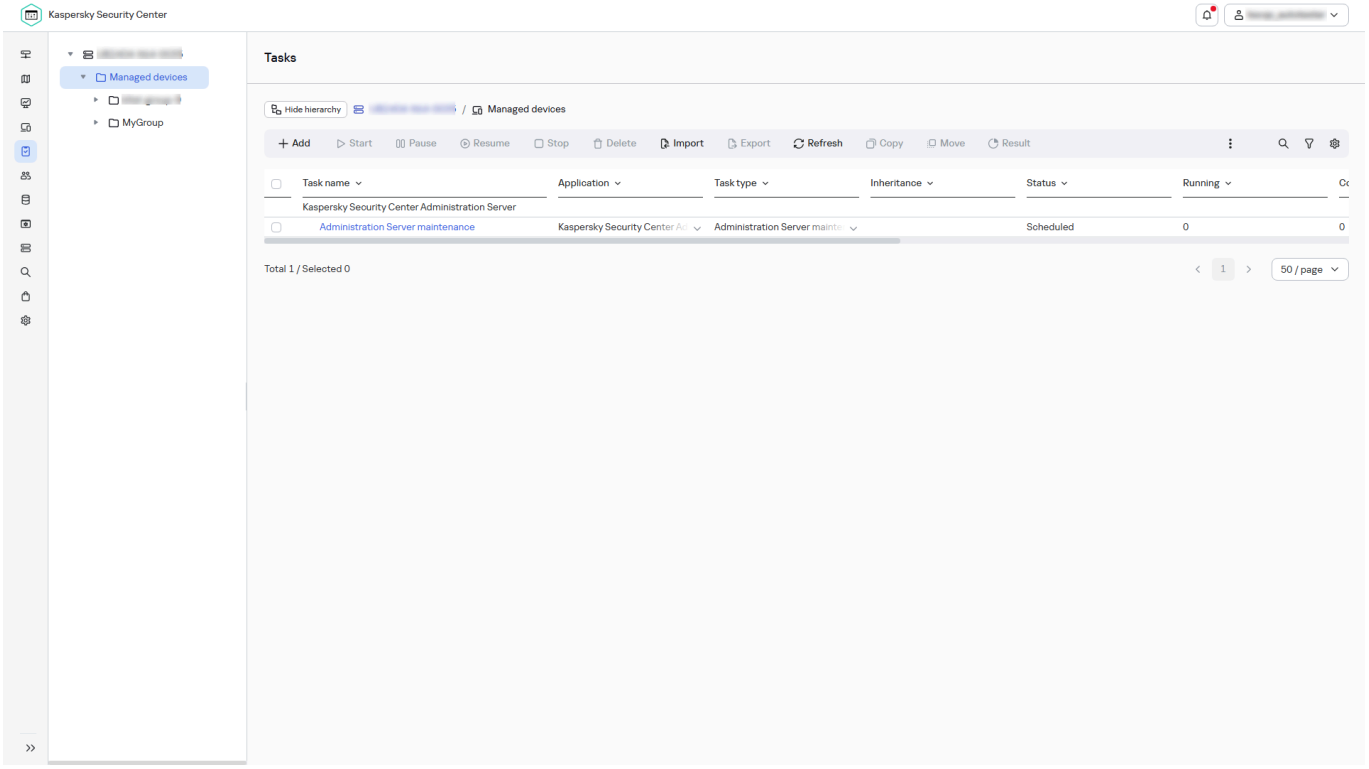
This task is required to download updates from Kaspersky update servers to the repositories of distribution points. The list of updates includes:

- Updates to databases and software modules for Kaspersky security applications
- Updates to Kaspersky Security Center components
- Updates to Kaspersky security applications

After the updates are downloaded, they can be propagated to the managed devices.

*To create the **Download updates to the repositories of distribution points** task, for a selected administration group:*

1. In the main menu, go to **Tasks**.



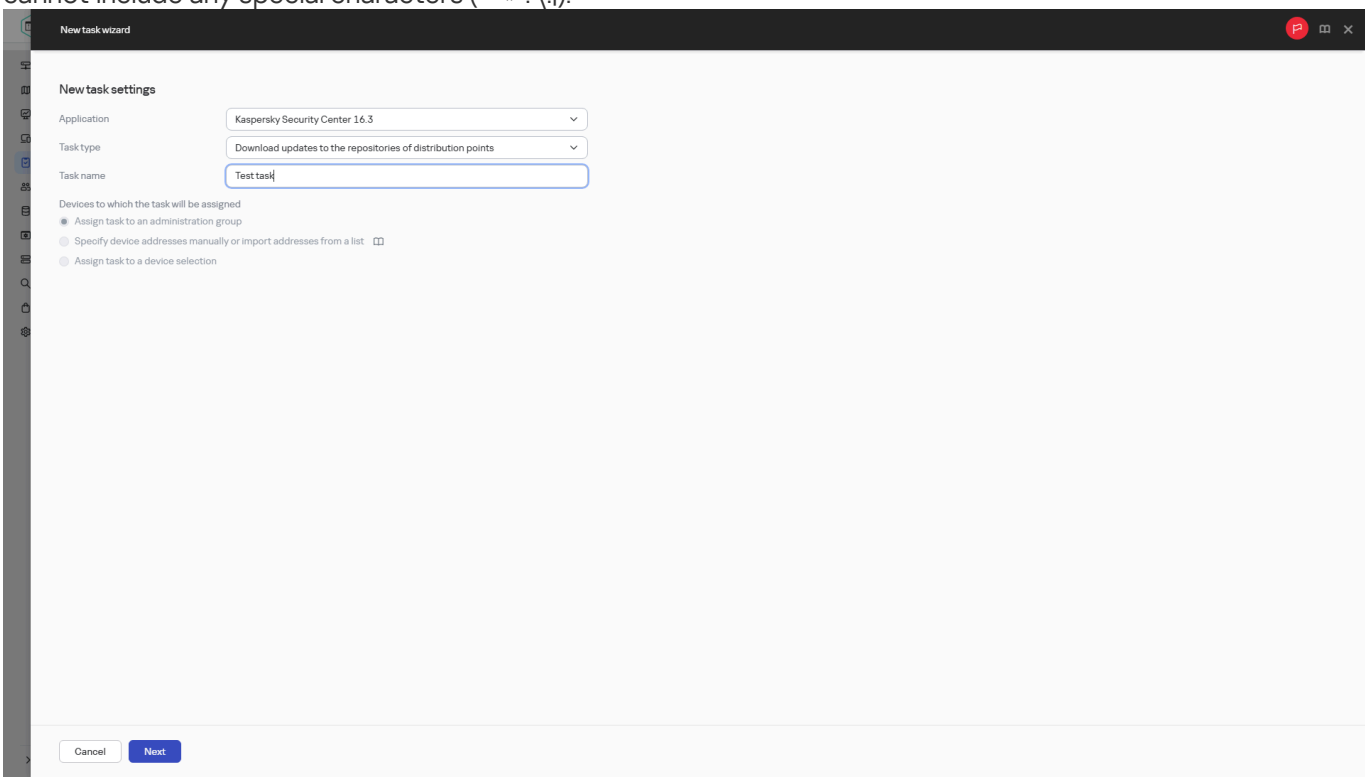

The Tasks section

2. Click **Add**.

   The New task wizard starts. Follow the steps of the wizard.

3. For the Kaspersky Security Center application, in the **Task type** field select **Download updates to the repositories of distribution points**.

4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).




Creating the Download updates to the repositories of distribution points task

5. Select an option button to specify the administration group, the device selection, or the devices to which the task applies.

6. At the **Finish task creation** step, if you want to modify the default task settings, enable the **Open task details when creation is complete** option. If you do not enable this option, the task will be created with the default settings. You can change the default settings later, at any time.

7. Click **Create**.

   The task is created and displayed in the list of tasks.

8. Click the name of the created task to open the task properties window.

9. On the **Application settings** tab of the task properties window, specify the following settings:

   **Sources of updates**

   The following resources can be used as a source of updates for the distribution point:

   - Kaspersky update servers

     HTTP servers at Kaspersky from which Kaspersky applications download database and application module updates.

     This option is selected by default.

   - Local or network folder

     A local or network folder that contains the latest updates. Only a mounted SMB share can be used as a network folder. When selecting a local folder, you must specify a folder on the device that has Administration Server installed.

In the *Download updates to the Administration Server repository* task and the *Download updates to the repositories of distribution points* task, user authentication does not work if you select a password-protected local or network folder as an update source. To resolve this issue, first mount the password-protected folder, and then specify the required credentials, for example, by means of the operating system. After that, you can select this folder as an update source in an update download task. Kaspersky Security Center Linux will not require that you enter the credentials.

**Folder for storing updates**

The path to the specified folder for storing saved updates. You can copy the specified folder path to a clipboard. You cannot change the path to a specified folder for a group task.

**Download diff files**

This option enables the downloading diff files feature.

By default, this option is disabled.

**Download updates by using the old scheme**

Starting from version 14, Kaspersky Security Center downloads updates of databases and software modules by using the new scheme. For the application to download updates by using the new scheme, the update source must contain the update files with the metadata compatible with the new scheme. If the update source contains the update files with the metadata compatible with the old scheme only, enable the **Download updates by using the old scheme** option. Otherwise, the update download task will fail.

For example, you must enable this option when a local or network folder is specified as an update source and the update files in this folder were downloaded by one of the following applications:

- Kaspersky Update Utility

  This utility downloads updates by using the old scheme.

- Kaspersky Security Center 13 Linux

  For example, a distribution point is configured to take the updates from a local or network folder. In this case, you may download updates by using an Administration Server that has an internet connection, and then place the updates to the local folder on the distribution point. If the Administration Server has version 13, enable the **Download updates by using the old scheme** option in the *Download updates to the repositories of distribution points* task.

By default, this option is disabled.

10. Create a schedule for task start. If necessary, configure the following settings:

- **Start task**:

  **Manually** (selected by default)

  The task does not run automatically. You can only start it manually.

  By default, this option is selected.

  **Every N minutes**

  The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

  By default, the task runs every 30 minutes, starting from the current system time.

  **Every N hours**

  The task runs regularly, with the specified interval in hours, starting from the specified date and time.

By default, the task runs every 6 hours, starting from the current system date and time.

**Every N days**

The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

By default, the task runs every day, starting from the current system date and time.

**By days of week**

The task runs regularly, on the specified days of the week, at the specified time.

By default, the task runs every Friday at 6:00:00 PM.

**Monthly**

The task runs regularly, on the specified day of the month, at the specified time.

In months that lack the specified day, the task runs on the last day.

By default, the task runs on the first day of each month, at the current system time.

**Monthly on selected weekday**

The task runs regularly, on the specified days of each month, at the specified time.

By default, the start time is 18:00, and no days of the month are selected.

> Note that you select neither a specific date in the month, nor the number of the week (first, second week of the month) but the sequence number of the weekday within a month. For example, if you set the cursor in the **Tu** cell of the **First** row, it means the task will run every first Tuesday of each new month.

You can select several days of week.

**On virus outbreak**

The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

- Anti-virus for workstations and file servers
- Anti-virus for perimeter defense
- Anti-virus for mail systems

By default, all application types are selected.

You may want to run different tasks depending on the security application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

**On completing another task**

The current task starts after another task completes. This option only works if both tasks are assigned to the same devices. For example, you may want to run the *Manage devices* task with the **Turn on the device** option and, after it completes, run the *Virus scan* task as a triggering task.

You have to select the triggering task from the table and the status with which this task must complete (**Completed successfully** or **Failed**).

If necessary, you can search, sort, and filter the tasks in the table as follows:

- Enter the task name in the search field, to search the task by its name.
- Click the sort icon to sort the tasks by name.

  By default, the tasks are sorted in alphabetical ascending order.
- Click the filter icon, and in the window that opens, filter the tasks by group, and then click the **Apply** button.

- **Run missed tasks**

  This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

  If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

  If this option is disabled, only scheduled tasks run on client devices. For **Manually**, **Once** and **Immediately** schedule, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

  By default, this option is enabled.

- **Use automatically randomized delay for task starts**

  If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

  The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However, when task settings are edited or the task is started manually, the calculated value of the task start time changes.

  If this option is disabled, the task starts on client devices according to the schedule.

  By default, this option is enabled.

- **Use automatically randomized delay for task starts within an interval of**

  If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

  If this option is disabled, the task starts on client devices according to the schedule.

  By default, this option is disabled. The default time interval is one minute.

11. Click the **Save** button.

The task is created and configured.

In addition to the settings that you specify during task creation, you can change other properties of a created task.

When the *Download updates to the repositories of distribution points* task is performed, updates for databases and software modules are downloaded from the update source and stored in the shared folder. Downloaded updates will only be used by distribution points that are included in the specified administration group and that have no update download task explicitly set for them.

# Adding sources of updates for the Download updates to the Administration Server repository task

When you create or use the task for downloading updates to the Administration Server repository, you can choose the following sources of updates:

- Kaspersky update servers
- Primary Administration Server

  This resource applies to tasks created for a secondary or virtual Administration Server.
- Local or network folder

> In the *Download updates to the Administration Server repository* task and the *Download updates to the repositories of distribution points* task, user authentication does not work if you select a password-protected local or network folder as an update source. To resolve this issue, first mount the password-protected folder, and then specify the required credentials, for example, by means of the operating system. After that, you can select this folder as an update source in an update download task. Kaspersky Security Center Linux will not require that you enter the credentials.

Kaspersky update servers are used by default, but you can also download updates from a local or network folder. You might want to use the folder if your network does not have access to the internet. In this case, you can manually download updates from Kaspersky update servers and put the downloaded files in the necessary folder. You can specify only one path to a local or network folder.

When selecting a local folder, you must specify a folder on the device that has Administration Server installed. The path to the folder depends on the device's operating system. Since the local folder is located on Linux-based Administration Server, you have to specify the POSIX path, for example: /path/to/dir.

Only a mounted SMB share can be used as a network folder. If an SMB share requires authentication, it must be mounted in the system with the required credentials in advance. We recommend not using the SMB1 protocol since it is insecure.

*To add the sources of updates:*

1. In the main menu, go to **Tasks**.
2. Click **Download updates to the Administration Server repository**.
3. Go to the **Application settings** tab.
4. In the **Sources of updates** table, click the **Add** button.
5. In the window that opens, add the necessary sources, and then click the **Save** button.

   If you select the **Local or network folder** check box, specify a path to the folder.
6. Click the **Save** button in the task window.

Now updates are downloaded to the Administration Server repository from the specified sources.

If you add both Kaspersky update servers and the local or network folder, you can set priorities for the updates. To do this, in the **Sources of updates** table, select the check box next to the update for which you want to change the priority, and then click either **Move up** or **Move down** button.

# Approving and declining software updates

The settings of an update installation task may require approval of updates that are to be installed. You can approve updates that must be installed and decline updates that must not be installed.

For example, you may want to first check the installation of updates in a test environment and make sure that they do not interfere with the operation of devices, and only then allow the installation of these updates on client devices.

Approving and declining updates is available only for Network Agent and managed applications installed on the Windows-based client devices. Seamless updating of Administration Server, Kaspersky Security Center Web Console, and management web plug-ins is not supported. To update these components, you have to download the latest versions from the Kaspersky website, and then install them manually.

*To approve or decline one or several updates:*

1. In the main menu, go to **Software management** → **Kaspersky applications** → **Seamless updates**.

   A list of available updates appears.

   Updates of managed applications may require a specific minimum version of Kaspersky Security Center to be installed. If this version is later than your current version, these updates are displayed but cannot be approved. Also, no installation packages can be created from such updates until you upgrade Kaspersky Security Center. You are prompted to upgrade your Kaspersky Security Center instance to the required minimum version.

2. If necessary, accept EULA by clicking the **View and accept License Agreements** button.

3. Select the updates that you want to approve or decline.

4. Click **Approve** to approve the selected updates or **Decline** to decline the selected updates.

   The default value is *Undefined*.

The updates to which you assign *Approved* status are placed in a queue for installation.

The updates to which you assign *Declined* status are uninstalled (if possible) from all devices on which they were previously installed. Also, they will not be installed on other devices in future.

Some updates for Kaspersky applications cannot be uninstalled. If you set *Declined* status for them, Kaspersky Security Center Linux will not uninstall these updates from the devices on which they were previously installed. However, these updates will never be installed on other devices in future.

If you set *Declined* status for third-party software updates, these updates will not be installed on devices for which they were planned but have not yet been installed. Updates will remain on devices on which they were already installed. If you have to delete the updates, you can manually delete them locally.

# Automatic installation of updates for Kaspersky Endpoint Security for Windows

You can configure automatic updates of databases and software modules of Kaspersky Endpoint Security for Windows on client devices.

*To configure download and automatic installation of updates of Kaspersky Endpoint Security for Windows on devices:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts. Follow the instructions of the wizard.
3. For the Kaspersky Endpoint Security for Windows application, select **Update** as the task subtype.
4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).
5. Choose the task scope.
6. Specify the administration group, the device selection, or the devices to which the task applies.
7. At the **Finish task creation** step, if you want to modify the default task settings, enable the **Open task details when creation is complete** option. If you do not enable this option, the task will be created with the default settings. You can change the default settings later, at any time.
8. Click **Create**.

   The task is created and displayed in the list of tasks.
9. Click the name of the created task to open the task properties window.

10. On the **Application settings** tab of the task properties window, define the update task settings in local or mobile mode:

    - **Local mode**: Connection is established between the device and the Administration Server.
    - **Mobile mode**: No connection is established between Kaspersky Security Center Linux and the device (for example, when the device is not connected to the internet).

11. Enable the update sources that you want to use to update databases and application modules for Kaspersky Endpoint Security for Windows. If required, change positions of the sources in the list by using the **Move up** and **Move down** buttons. If several update sources are enabled, Kaspersky Endpoint Security for Windows tries to connect to them one after another, starting from the top of the list, and performs the update task by retrieving the update package from the first available source.

12. Enable the **Install approved application module updates** option to download and install software module updates together with the application databases.

    If the option is enabled, Kaspersky Endpoint Security for Windows notifies the user about available software module updates and includes software module updates in the update package when running the update task. Kaspersky Endpoint Security for Windows installs only those updates for which you have set the *Approved* status; they will be installed locally through the application interface or through Kaspersky Security Center Linux.

    You can also enable the **Automatically install critical application module updates** option. If any updates are available for software modules, Kaspersky Endpoint Security for Windows automatically installs those that have *Critical* status; the remaining updates will be installed after you approve them.

    If updating the software module requires reviewing and accepting the terms of the License Agreement and Privacy Policy, the application installs updates after the terms of the License Agreement and Privacy Policy have been accepted by the user.

13. Select the **Copy updates to folder** check box in order for the application to save downloaded updates to a folder, and then specify the folder path.

14. Schedule the task. To ensure timely updates, we recommend that you select the **When new updates are downloaded to the repository** option.

15. Click the **Save** button.

When the **Update** task is running, the application sends requests to Kaspersky update servers.

Some updates require installation of the latest versions of management plug-ins.

# About using diff files for updating Kaspersky databases and software modules

When Kaspersky Security Center Linux downloads updates from Kaspersky update servers, it optimizes traffic by using diff files. You can also enable the usage of diff files by devices (Administration Servers, distribution points, and client devices) that take updates from other devices on your network.

### About the Downloading diff files feature

A diff file describes the differences between two versions of a file of a database or software module. The usage of diff files saves traffic inside your company's network because diff files occupy less space than entire files of databases and software modules. If the *Downloading diff files* feature is enabled on Administration Server or a distribution point, the diff files are saved on this Administration Server or distribution point. As a result, devices that take updates from this Administration Server or distribution point can use the saved diff files to update their databases and software modules.

To optimize the usage of diff files, we recommend that you synchronize the update schedule of devices with the update schedule of the Administration Server or distribution point from which the devices take updates. However, the traffic can be saved even if devices are updated several times less often than are the Administration Server or distribution point from which the devices take updates.

Distribution points do not use IP multicasting for automatic distribution of diff files.

# Enabling the Downloading diff files feature

### Stages

1. **Enabling the feature on Administration Server**

   Enable the feature in the settings of a *Download updates to the repository of the Administration Server* task.

2. **Enabling the feature for a distribution point**

   Enable the feature for a distribution point that receives updates by means of a *Download updates to the repositories of distribution points* task.

   Then enable the feature in the Network Agent policy settings for a distribution point that receives updates from Administration Server.

   Then enable the feature for a distribution point that receives updates from Administration Server.

   The feature is enabled in the Network Agent policy settings and—if the distribution points are assigned manually and if you want to override policy settings—in the **Distribution points** section of the Administration Server properties.

To check that the Downloading diff files feature is successfully enabled, you can measure the internal traffic before and after you perform the scenario.

# Downloading updates by distribution points

Kaspersky Security Center Linux allows distribution points to receive updates from the Administration Server, Kaspersky servers, or from a local or network folder.

*To configure update download for a distribution point:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Distribution points** section.

3. Click the name of the distribution point through which updates will be delivered to client devices in the group.

4. In the distribution point properties window, select the **Source of updates** section.

5. Select an update source for the distribution point:

   **Source of updates**

   Select an update source for the distribution point:

   - To allow the distribution point to receive updates from the Administration Server, select **Retrieve from Administration Server**.

   - To allow the distribution point to receive updates by using a task, select **Use update download task**, and then specify a *Download updates to the repositories of distribution points* task:

     - If such a task already exists on the device, select the task in the list.

     - If no such task yet exists on the device, click the **Create task** link to create a task. The New task wizard starts. Follow the steps of the wizard.

   **Download diff files**

   This option enables the downloading diff files feature.

   By default, this option is enabled.

The distribution point will receive updates from the specified source.

# Updating Kaspersky databases and software modules on offline devices

Updating Kaspersky databases and software modules on managed devices is an important task for maintaining protection of the devices against viruses and other threats. Administrators usually configure regular updates through usage of the Administration Server repository.

When you need to update databases and software modules on a device (or a group of devices) that is not connected to the Administration Server (primary or secondary), a distribution point or the internet, you have to use alternative sources of updates, such as an FTP server or a local folder. In this case, you have to deliver the files of the required updates by using a mass storage device, such as a flash drive or an external hard drive.

You can copy the required updates from:

- The Administration Server.

  To be sure the Administration Server repository contains the updates required for the security application installed on an offline device, at least one of the managed online devices must have the same security application installed. This application must be configured to receive the updates from the Administration Server repository through the *Download updates to the Administration Server repository* task.

- Any device that has the same security application installed and configured to receive the updates from the Administration Server repository, a distribution point repository, or directly from the Kaspersky update servers.

Below is an example of configuring updates of databases and software modules by copying them from the Administration Server repository.

*To update Kaspersky databases and software modules on offline devices:*

1. Connect the removable drive to the device where the Administration Server is installed.

2. Copy the updates files to the removable drive.

   By default, the updates are located at: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   Alternatively, you can configure Kaspersky Security Center Linux to regularly copy the updates to the folder that you select. For this purpose, use the **Copy downloaded updates to additional folders** option in the properties of the *Download updates to the Administration Server repository* task. If you specify a folder located on a flash drive or an external hard drive as a destination folder for this option, this mass storage device will always contain the latest version of the updates.

3. On offline devices, configure Kaspersky Endpoint Security to receive updates from a local folder or a shared resource, such as an FTP server or a shared folder.

   How-to instructions:

   - Kaspersky Endpoint Security for Linux Help
   - Kaspersky Endpoint Security for Windows Help

4. Copy the updates files from the removable drive to the local folder or the shared resource that you want to use as an update source.

5. On the offline device that requires update installation, start the *Update* task of Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Windows, depending on the operating system of the offline device.

After the update task is complete, the Kaspersky databases and software modules are up-to-date on the device.

# Monitoring, reporting, and audit

This section describes the monitoring and reporting capabilities of Kaspersky Security Center Linux. These capabilities give you an overview of your infrastructure, protection statuses, and statistics.

After Kaspersky Security Center Linux deployment or during the operation, you can configure the monitoring and reporting features to best suit your needs.

# Scenario: Monitoring and reporting

This section provides a scenario for configuring the monitoring and reporting feature in Kaspersky Security Center Linux.

## Prerequisites

After you deploy Kaspersky Security Center Linux in an organization's network, you can start to monitor it and generate reports on its functioning.

Monitoring and reporting in an organization's network proceeds in stages:

1. **Configuring the switching of device statuses**

   Get acquainted with the settings for device statuses depending on specific conditions. By changing these settings, you can change the number of events with *Critical* or *Warning* importance levels. When configuring the switching of device statuses, be sure of the following:

   - New settings do not conflict with the information security policies of your organization.
   - You are able to react to important security events in your organization's network in a timely manner.

2. **Configuring notifications about events on client devices**

   How-to instructions:

   **Configure notification (by email, by SMS, or by running an executable file) of events on client devices**

3. **Performing recommended actions for Critical and Warning notifications**

   How-to instructions:

   **Perform recommended actions for your organization's network**

4. **Reviewing the security status of your organization's network**

   How-to instructions:

   - Review the Protection status widget
   - Generate and review the Report on protection status
   - Generate and review the Report on errors

5. **Locating client devices that are not protected**

   How-to instructions:

   - Review the New devices widget
   - Generate and review the Report on protection deployment

6. **Checking protection of client devices**

   How-to instructions:

   - Generate and review reports from the Protection status and Threat statistics categories
   - Start and review the Critical event selection

7. **Evaluating and limiting the event load on the database**

   Information about events that occur during operation of managed applications is transferred from a client device and registered in the Administration Server database. To reduce the load on the Administration Server, evaluate and limit the maximum number of events that can be stored in the database.

   How-to instructions:

   - Limiting the maximum number of events

8. **Reviewing license information**

   How-to instructions:

   - Add the License key usage widget to the dashboard and review it
   - Generate and review the Report on usage of license keys

Results

Upon completion of the scenario, you are informed about protection of your organization's network and, thus, can plan actions for further protection.

# About types of monitoring and reporting

Information on security events in an organization's network is stored in the Administration Server database. Based on the events, Kaspersky Security Center Web Console provides the following types of monitoring and reporting in your organization's network:

- Dashboard
- Reports
- Event selections
- Notifications

### Dashboard

The dashboard allows you to monitor security trends on your organization's network by providing you with a graphical display of information.

### Reports

The Reports feature allows you to get detailed numerical information about the security of your organization's network, save this information to a file, send it by email, and print it.

### Event selections

Event selections provide an onscreen view of named sets of events that are selected from the Administration Server database. These sets of events are grouped according to the following categories:

- By importance level—**Critical events**, **Functional failures**, **Warnings**, and **Info events**
- By time—**Recent events**
- By type—**User requests** and **Audit events**

You can create and view user-defined event selections based on the settings available, in the Kaspersky Security Center Web Console interface, for configuration.

### Notifications

Notifications alert you about events and help you to speed up your responses to these events by performing recommended actions or actions you consider as appropriate.

# Triggering of rules in Smart Training mode

This section provides information about the detections performed by the Adaptive Anomaly Control rules in Kaspersky Endpoint Security for Windows on client devices.

The rules detect anomalous behavior on client devices and may block it. If the rules work in Smart Training mode, they detect anomalous behavior and send reports about every such occurrence to Administration Server. You can view the reports about detected anomalous behavior in **Repositories → Rule triggers in Smart Training state**. You can confirm detections as correct or add them as exclusions, so that this type of behavior is not considered anomalous anymore.

Information about detections is stored in the event log on the Administration Server (along with other events) and in the Adaptive Anomaly Control report.

For more information about Adaptive Anomaly Control, the rules, their modes and statuses, refer to Kaspersky Endpoint Security for Windows Help.

# Viewing and confirming detections performed using Adaptive Anomaly Control rules

*To view the list of detections performed by Adaptive Anomaly Control rules:*

1. In the main menu, go to **Repositories → Rule triggers in Smart Training state**.

   The list displays the following information about detections performed using Adaptive Anomaly Control rules:

   - **Administration group**

     The name of the administration group where the device belongs.

   - **Virtual Administration Server**

     Virtual Administration Server that manages the device.

   - **Device name**

     The name of the client device where the rule was applied.

   - **Name**

     The name of the rule that was applied.

   - **Status**

     **Excluding**—If the Administrator processed this item and added it as an exclusion to the rules. This status remains till the next synchronization of the client device with the Administration Server; after the synchronization, the item disappears from the list.

     **Confirming**—If the Administrator processed this item and confirmed it. This status remains till the next synchronization of the client device with the Administration Server; after the synchronization, the item disappears from the list.

     Empty—If the Administrator did not process this item.

   - **Detections count**

     The number of detects within one heuristic rule, one process and one client device. This number is counted by Kaspersky Endpoint Security.

   - **User name**

     The name of the client device user who run the process that generated the detect.

   - **Source process path**

     Path to the source process, i.e. to the process that performs the action (for more information, refer to the Kaspersky Endpoint Security help).

   - **Source process hash**

     SHA256 hash of the source process file (for more information, refer to the Kaspersky Endpoint Security help).

- **Source object path**

  Path to the object that started the process (for more information, refer to the Kaspersky Endpoint Security help).

- **Source object hash**

  SHA256 hash of the source file (for more information, refer to the Kaspersky Endpoint Security help).

- **Target process path**

  Path to the target process (for more information, refer to the Kaspersky Endpoint Security help).

- **Target process hash**

  SHA256 hash of the target file (for more information, refer to the Kaspersky Endpoint Security help).

- **Target object path**

  Path to the target object (for more information, refer to the Kaspersky Endpoint Security help).

- **Target object hash**

  SHA256 hash of the target file (for more information, refer to the Kaspersky Endpoint Security help).

- **Processed**

  Date when the anomaly was detected.

*To view the properties of a detection:*

1. In the main menu, go to **Repositories** → **Rule triggers in Smart Training state**.
2. Do one of the following:

   - In the **Name** column, click the link with the name of the detection you want to view.
   - In the list of detections, select the check box next to the detection you want to view, and then click the **Properties** button.

   The properties window of the selected detection opens, displaying information about it.

You can confirm any detection from the list of detections of Adaptive Anomaly Control rules or from the properties window of a selected detection.

*To confirm a detection:*

- Select one or several detections in the list of detections, and then click the **Confirm** button.
- Open the properties window of a selected detection, and then click the **Confirm** button.

  The status of the detection is changed to **Confirming**. The detection disappears from the list of detections after the next synchronization of the client device with the Administration Server.

  Your confirmation will contribute to the statistics used by the rules. For more information, refer to Kaspersky Endpoint Security for Windows Help.

## Adding exclusions from the Adaptive Anomaly Control rules

The Add to Adaptive Anomaly Control exclusions wizard allows you to add exclusions from the Adaptive Anomaly Control rules for Kaspersky Endpoint Security.

*To add exclusions from the Adaptive Anomaly Control rules by using the wizard:*

1. Start the wizard in one of the following ways:

   - In the main menu, go to **Repositories → Rule triggers in Smart Training state**, select one or several detections, and then click the **Exclude** button.

     You can add up to 1000 exclusions at a time.

     Before adding a detection to exclusions, you can view the properties of the detection by clicking the detection name or the **Properties** button. In the detection properties window that opens, you can also click the **Exclude** button.

   - In the main menu, go to the **Monitoring → Event selections**, click the link with the event selection you need, select the check box next to the detection you want to exclude, and then click the **Exclude from Adaptive Anomaly Control** button.

   The Add to Adaptive Anomaly Control exclusions wizard starts. Proceed through the wizard by using the **Next** button.

2. Select the policies and profiles to which you want to add exclusions.

   Inherited policies cannot be updated. If you do not have the rights to modify a policy, the policy will not be updated.

3. Click **Done** to close the wizard.

The status of the detection is changed to **Excluding**. The detection disappears from the list of detections after the next synchronization of the client device with the Administration Server. The exclusion from the Adaptive Anomaly Control rules is configured and applied.

# Dashboard and widgets

This section contains information about the dashboard and the widgets that the dashboard provides. The section includes instructions on how to manage widgets and configure widget settings.

## Using the dashboard

The dashboard allows you to monitor security trends on your organization's network by providing you with a graphical display of information.

The dashboard is available in the Kaspersky Security Center Web Console, in the **Monitoring** section, by clicking **Dashboard**.

The dashboard provides widgets that can be customized. You can choose a large number of different widgets, presented as pie charts or donut charts, tables, graphs, bar charts, and lists. The information displayed in the widgets is automatically updated, the update period is from one to two minutes. The interval between updates varies for different widgets. You can refresh data on a widget manually at any time by means of the settings menu.

By default, widgets include information about all events stored in the database of Administration Server.

Kaspersky Security Center Web Console has a default set of widgets for the following categories:

- **Protection status**
- **Deployment**
- **Updating**
- **Threat statistics**
- **Other**

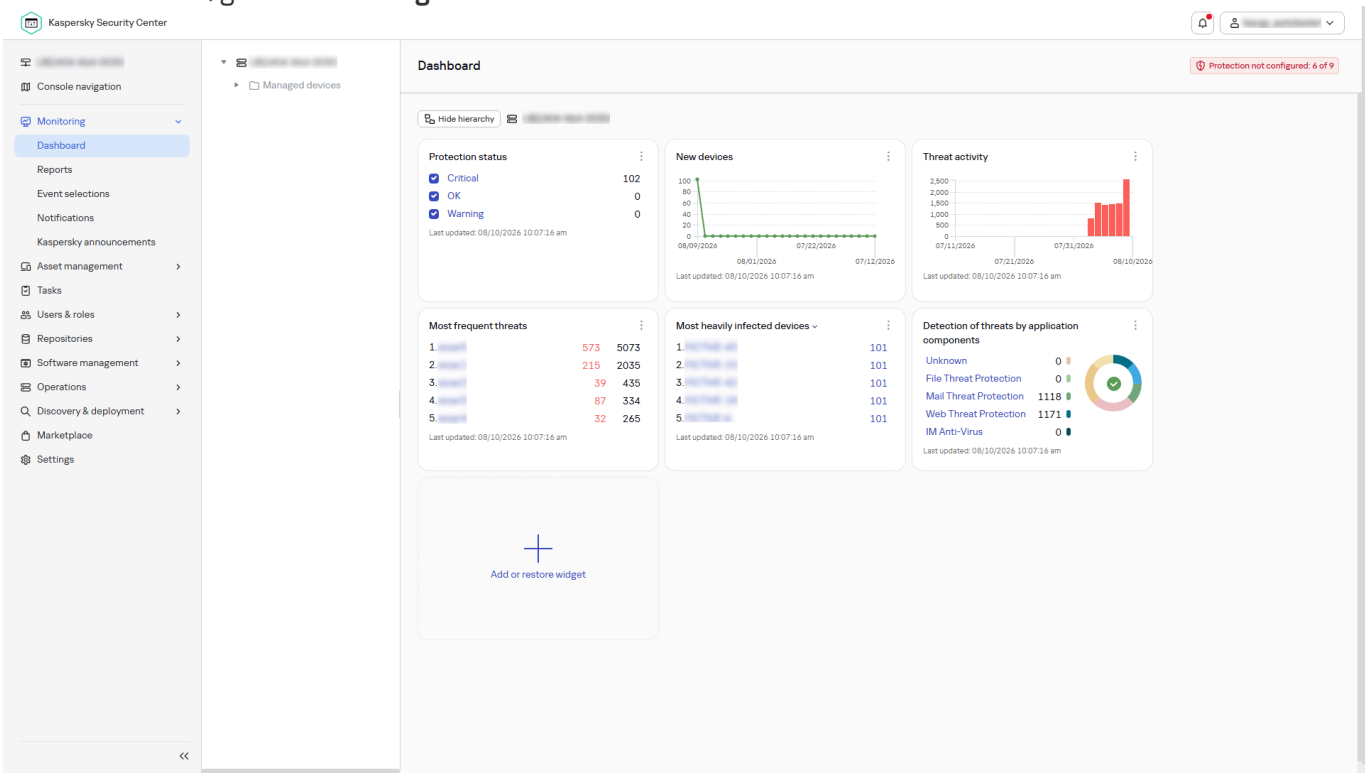
Some widgets have text information with links. You can view detailed information by clicking the link.

When configuring the dashboard, you can add widgets that you need, hide widgets that you do not need, change the size or appearance of widgets, move widgets, and change their settings.

# Adding widgets to the dashboard

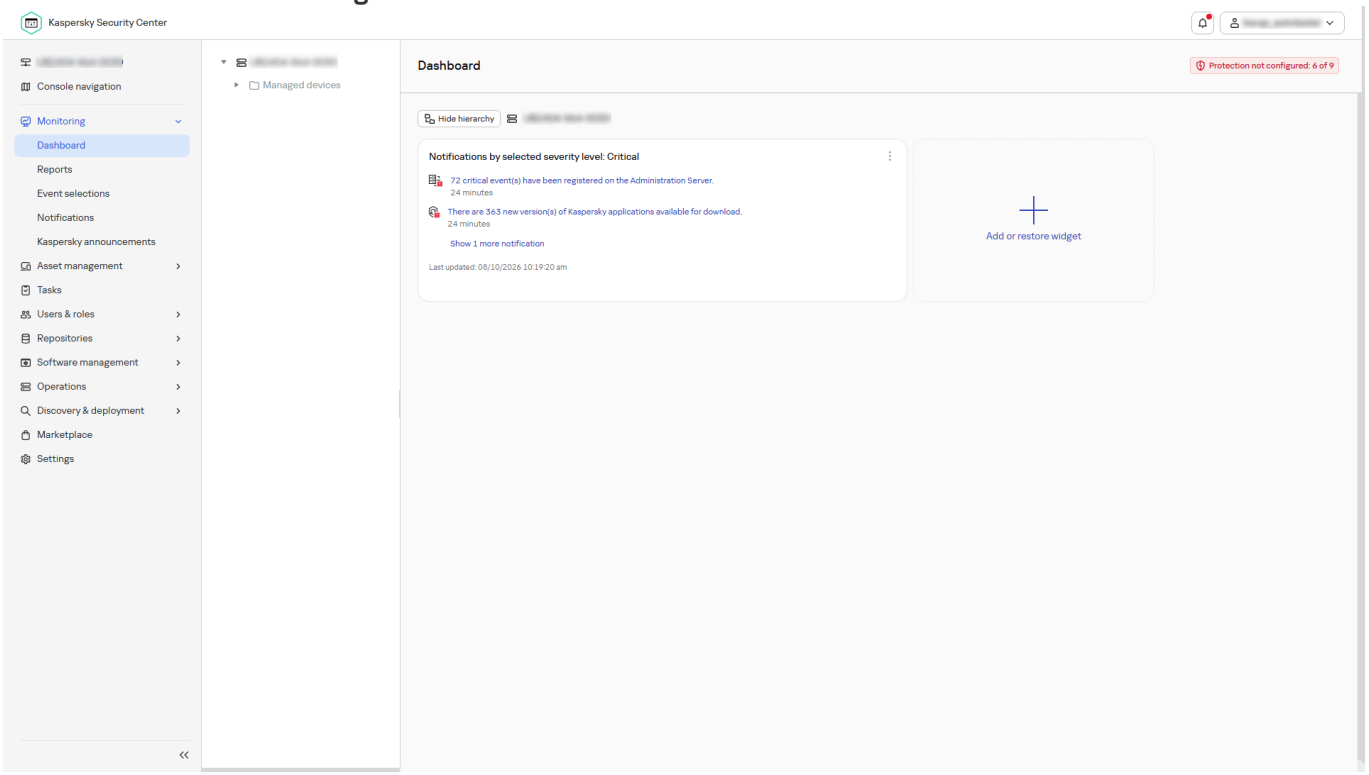
*To add widgets to the dashboard:*

1. In the main menu, go to **Monitoring** → **Dashboard**.




The dashboard with widgets

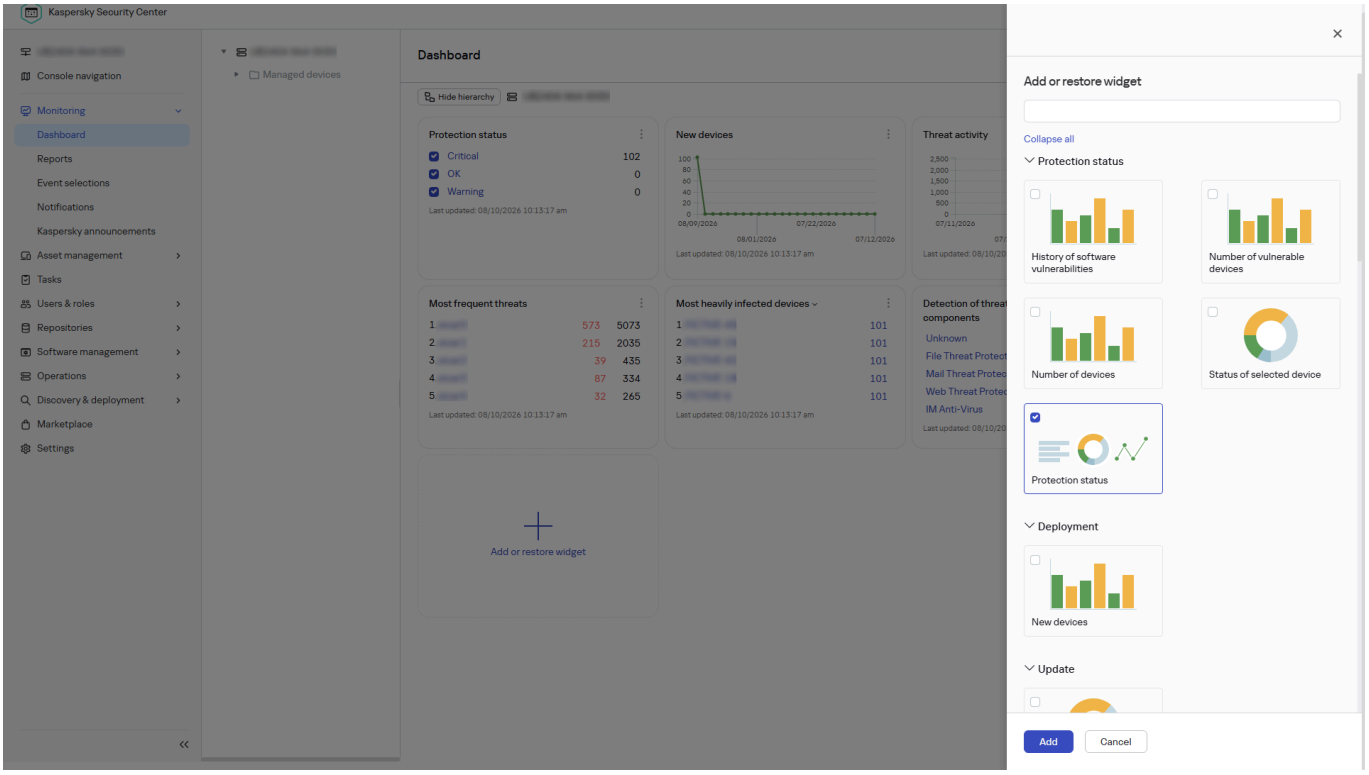
2. Click the **Add or restore widget** button.




Adding a widget

3. In the list of available widgets, select the widgets that you want to add to the dashboard.

   Widgets are grouped by category. To view the list of widgets included in a category, click the chevron icon (>) next to the category name.




Selecting the widget type

4. Click the **Add** button.

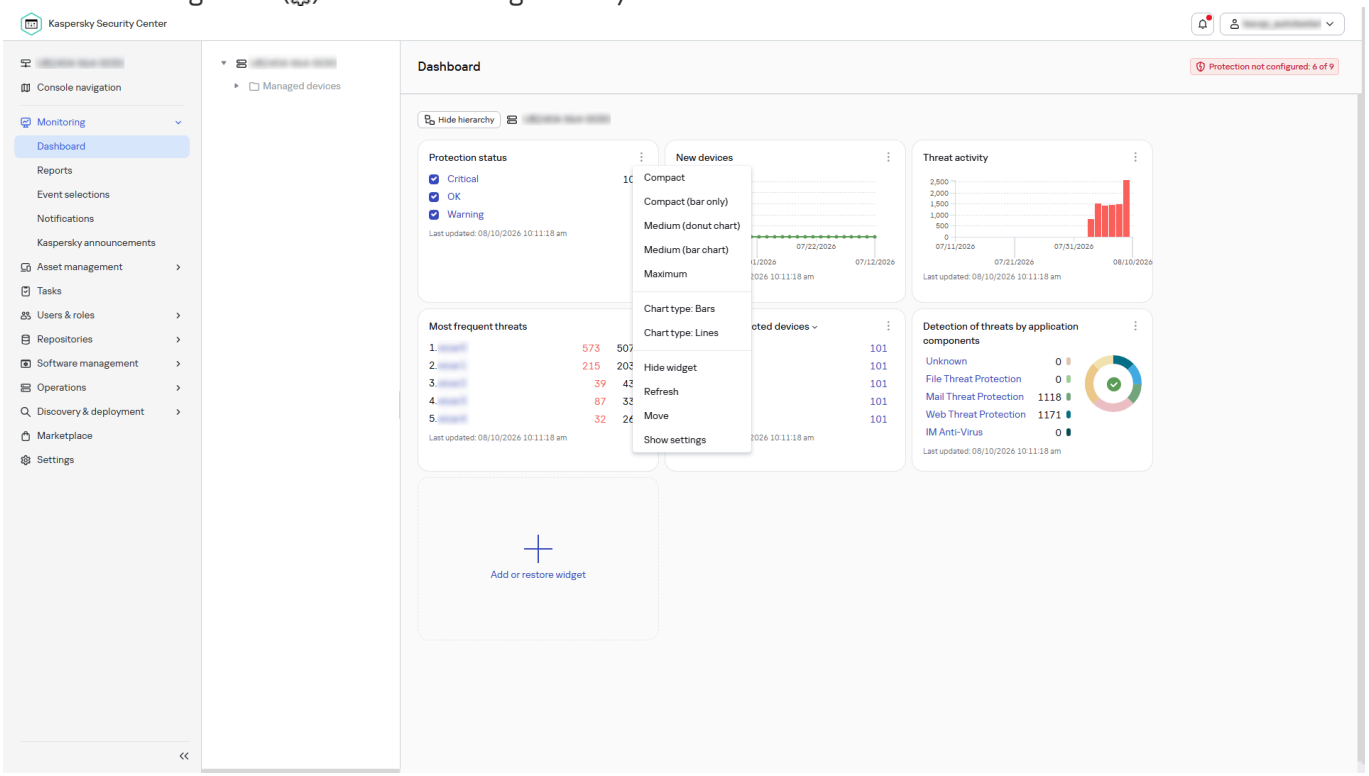
The selected widgets are added at the end of the dashboard.

You can now edit the representation and parameters of the added widgets.

# Hiding a widget from the dashboard

*To hide a displayed widget from the dashboard:*

1. In the main menu, go to the **Monitoring** → **Dashboard**.
2. Click the settings icon (⚙) next to the widget that you want to hide.




The widget menu

3. Select **Hide widget**.
4. In the **Warning** window that opens, click **OK**.

The selected widget is hidden. Later, you can add this widget to the dashboard again.

# Moving a widget on the dashboard

*To move a widget on the dashboard:*

1. In the main menu, go to **Monitoring** → **Dashboard**.
2. Click the settings icon (⚙) next to the widget that you want to move.

3. Select **Move**.

4. Click the place to which you want to move the widget. You can select only another widget.

The places of the selected widgets are swapped.

# Changing the widget size or appearance

For widgets that display a graph, you can change its representation—a bar chart or a line chart. For some widgets, you can change their size: compact, medium, or maximum.

*To change the widget representation:*

1. In the main menu, go to **Monitoring** → **Dashboard**.

2. Click the settings icon (⚙) next to the widget that you want to edit.

3. Do one of the following:

   - To display the widget as a bar chart, select **Chart type: Bars**.
   - To display the widget as a line chart, select **Chart type: Lines**.
   - To change the area occupied by the widget, select one of the values:
     - **Compact**
     - **Compact (bar only)**
     - **Medium (donut chart)**
     - **Medium (bar chart)**
     - **Maximum**

The representation of the selected widget is changed.

# Changing widget settings

*To change settings of a widget:*

1. In the main menu, go to **Monitoring** → **Dashboard**.

2. Click the settings icon (⚙) next to the widget that you want to change.

3. Select **Show settings**.

4. In the widget settings window that opens, change the widget settings as required.

5. Click **Save** to save changes.

The settings of the selected widget are changed.

The set of settings depends on the specific widget. Below are some of the common settings:

- **Widget scope** (the set of objects for which the widget displays information)—for example, an administration group or device selection.
- **Select task** sets the task for which the widget displays information.
- **Time interval** (the time interval during which the information is displayed in the widget)—between the two specified dates; from the specified date to the current day; or from the current day minus the specified number of days to the current day.
- The **Set to Critical if the following settings are specified** and **Set to Warning if the following settings are specified** rules govern how colors are assigned on the status chart.

After you change the widget settings, you can refresh data on the widget manually.

*To refresh data on a widget:*

1. In the main menu, go to **Monitoring** → **Dashboard**.
2. Click the settings icon (⚙) next to the widget that you want to move.
3. Select **Refresh**.

The data on the widget is refreshed.

# About the Dashboard-only mode

You can configure the Dashboard-only mode for employees who do not manage the network but who want to view the network protection statistics in Kaspersky Security Center Linux (for example, a top manager). When a user has this mode enabled, only a dashboard with a predefined set of widgets is displayed to the user. Thus, he or she can monitor the statistics specified in the widgets, for example, the protection status of all managed devices, the number of recently detected threats, or the list of the most frequent threats in the network.

When a user works in the Dashboard-only mode, the following restrictions are applied:

- The main menu is not displayed to the user, so he or she cannot change the network protection settings.
- The user cannot perform any actions with widgets, for example, add or hide them. Therefore, you need to put all widgets required for the user on the dashboard and configure them, for instance, set the rule of counting objects or specify the time interval.

You cannot assign the Dashboard-only mode to yourself. If you want to work in this mode, contact a system administrator, Managed Service Provider (MSP), or a user with the **Modify object ACLs** right in the **General features: User permissions** functional area.

# Configuring the Dashboard-only mode

Before you begin to configure the Dashboard-only mode, make sure that the following prerequisites are met:

- You have the **Modify object ACLs** right in the **General features: User permissions** functional area. If you do not have this right, the tab for configuring the mode will be missing.
- The user has the **Read** right in the **General features: Basic functionality** functional area.

If a hierarchy of Administration Servers is arranged in your network, for configuring the Dashboard-only mode go to the Server where the user account is available on the **Users** tab of the **Users & roles** → **Users & groups** section. It can be a primary Server or physical secondary Server. It is not possible to adjust the mode on a virtual server.

*To configure the Dashboard-only mode:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the user account name for which you want to adjust the dashboard with widgets.
3. In the account settings window that opens, select the **Dashboard** tab.

   On the tab that opens, the same dashboard is displayed for you as for the user.
4. If the **Display the console in Dashboard-only mode** option is enabled, switch the toggle button to disable it.

   When this option is enabled, you are also unable to change the dashboard. After you disable the option, you can manage widgets.
5. Configure the dashboard appearance. The set of widgets prepared on the **Dashboard** tab is available for the user with the customizable account. He or she cannot change any settings or size of the widgets, add, or remove any widgets from the dashboard. Therefore, adjust them for the user, so he or she can view the network protection statistics. To do this, on the **Dashboard** tab, you can perform the same actions with widgets as in the **Monitoring** → **Dashboard** section:
   - Add new widgets to the dashboard.
   - Hide widgets that the user doesn't need.
   - Move widgets into a specific order.
   - Change the size or appearance of widgets.
   - Change the widget settings.
6. Switch the toggle button to enable the **Display the console in Dashboard-only mode** option.

   After that, only the dashboard is available for the user. He or she can monitor statistics but cannot change the network protection settings and dashboard appearance. As the same dashboard is displayed for you as for the user, you are also unable to change the dashboard.

   If you keep the option disabled, the main menu is displayed for the user, so he or she can perform various actions in Kaspersky Security Center Linux, including changing security settings and widgets.

7. Click the **Save** button when you finish configuring the Dashboard-only mode. Only after that will the prepared dashboard be displayed to the user.

8. If the user wants to view statistics of supported Kaspersky applications and needs access rights to do so, configure the rights for the user. After that, Kaspersky applications data is displayed for the user in the widgets of these applications.

Now the user can log in to Kaspersky Security Center Linux under the customized account and monitor the network protection statistics in the Dashboard-only mode.

# Administration and protection reports

This section describes how to use reports, manage custom report templates, use report templates to generate new reports, and create report delivery tasks.

## Using reports

The Reports feature allows you to get detailed numerical information about the security of your organization's network, save this information to a file, send it by email, and print it.

Reports are available in the Kaspersky Security Center Web Console, in the **Monitoring** section, by clicking **Reports**.

By default, reports include information for the last 30 days.

Kaspersky Security Center Linux has a default set of reports for the following categories:

- **Protection status**
- **Deployment**
- **Updating**
- **Threat statistics**
- **Other**

You can create custom report templates, edit report templates, and delete them.

You can create reports that are based on existing templates, export reports to files, and create tasks for report delivery.

# Creating a report template

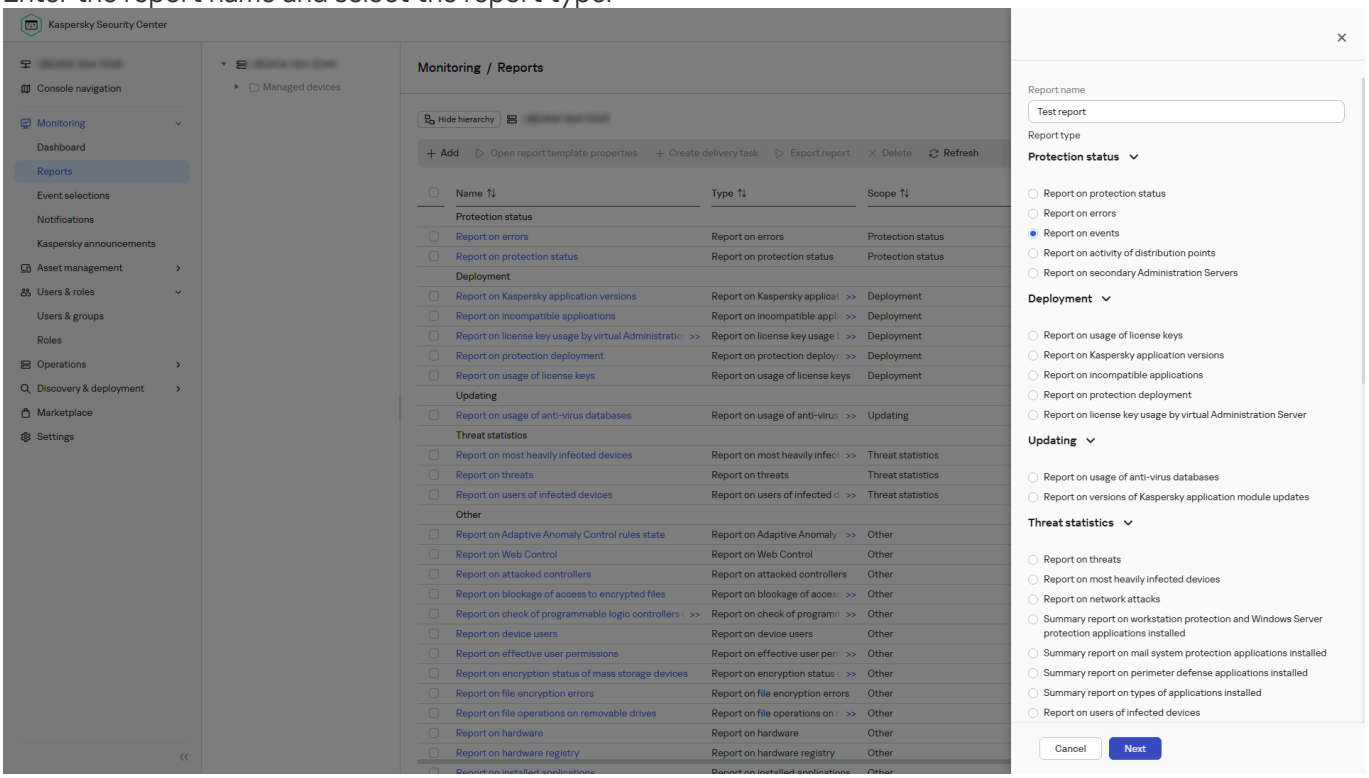
*To create report template:*

1. In the main menu, go to **Monitoring** → **Reports**.

2. Click **Add**.

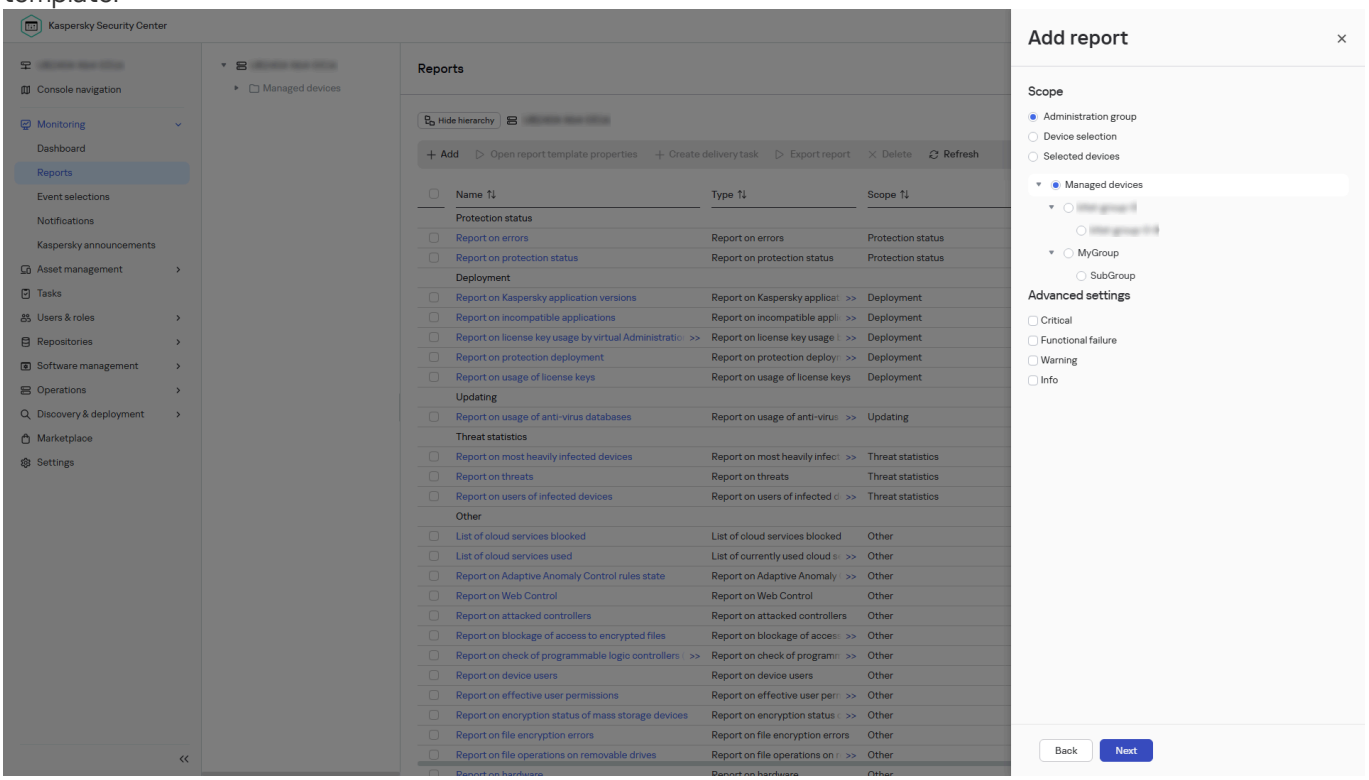
   The New report template wizard starts. Proceed through the wizard by using the **Next** button.

3. Enter the report name and select the report type.




Specifying the report name and selecting the report type

4. On the **Scope** step of the wizard, select the set of client devices (administration group, device selection, selected devices, or all networked devices) whose data will be displayed in reports that are based on this report template.

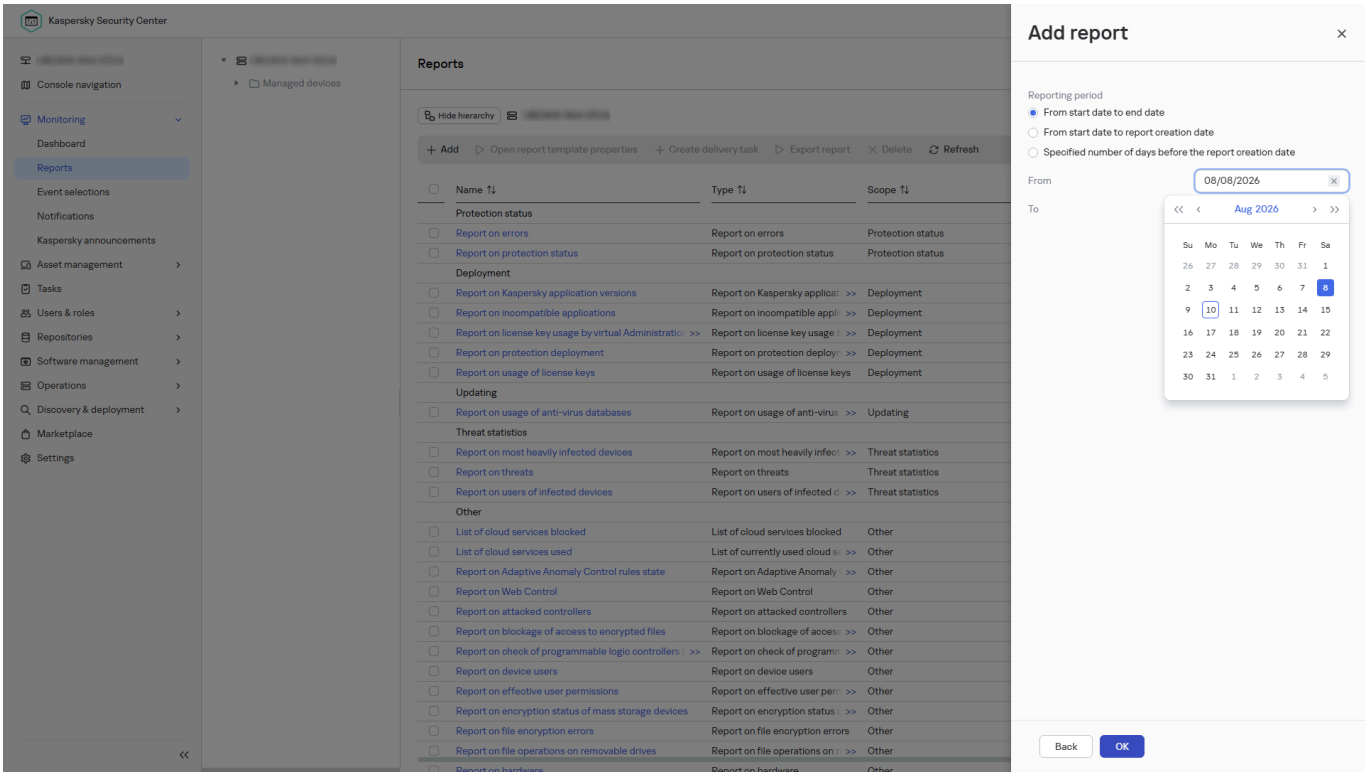



Specifying the report scope

5. On the **Reporting period** step of the wizard, specify the report period. Available values:

   - Between the two specified dates
   - From the specified date to the report creation date
   - From the report creation date, minus the specified number of days, to the report creation date

This page may not appear for some reports.




Specifying the reporting period

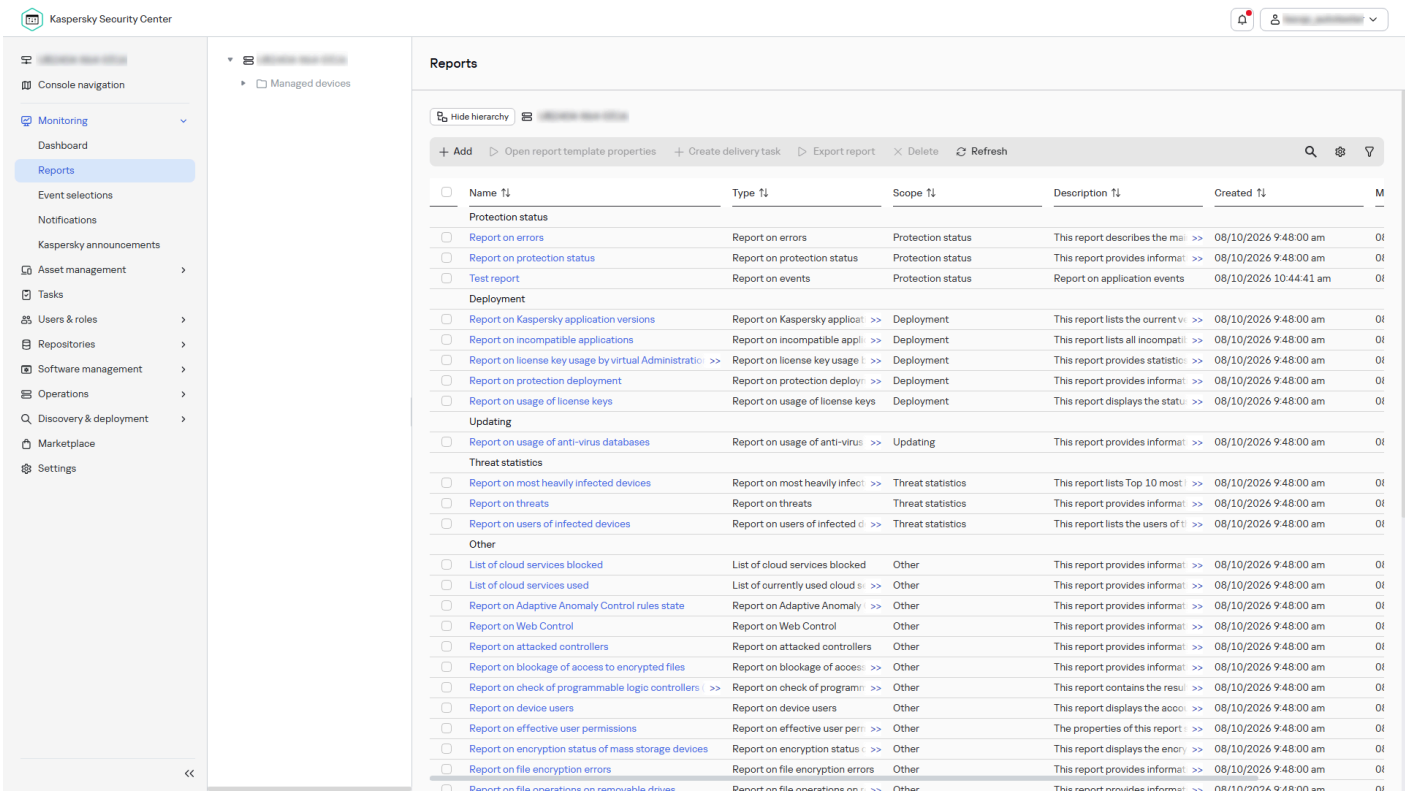
6. Click **OK** to close the wizard.

7. Do one of the following:

   - Click the **Save and run** button to save the new report template and to run a report based on it.
     The report template is saved. The report is generated.

   - Click the **Save** button to save the new report template.
     The report template is saved.

You can use the new template for generating and viewing reports.




The list of reports

# Viewing and editing report template properties

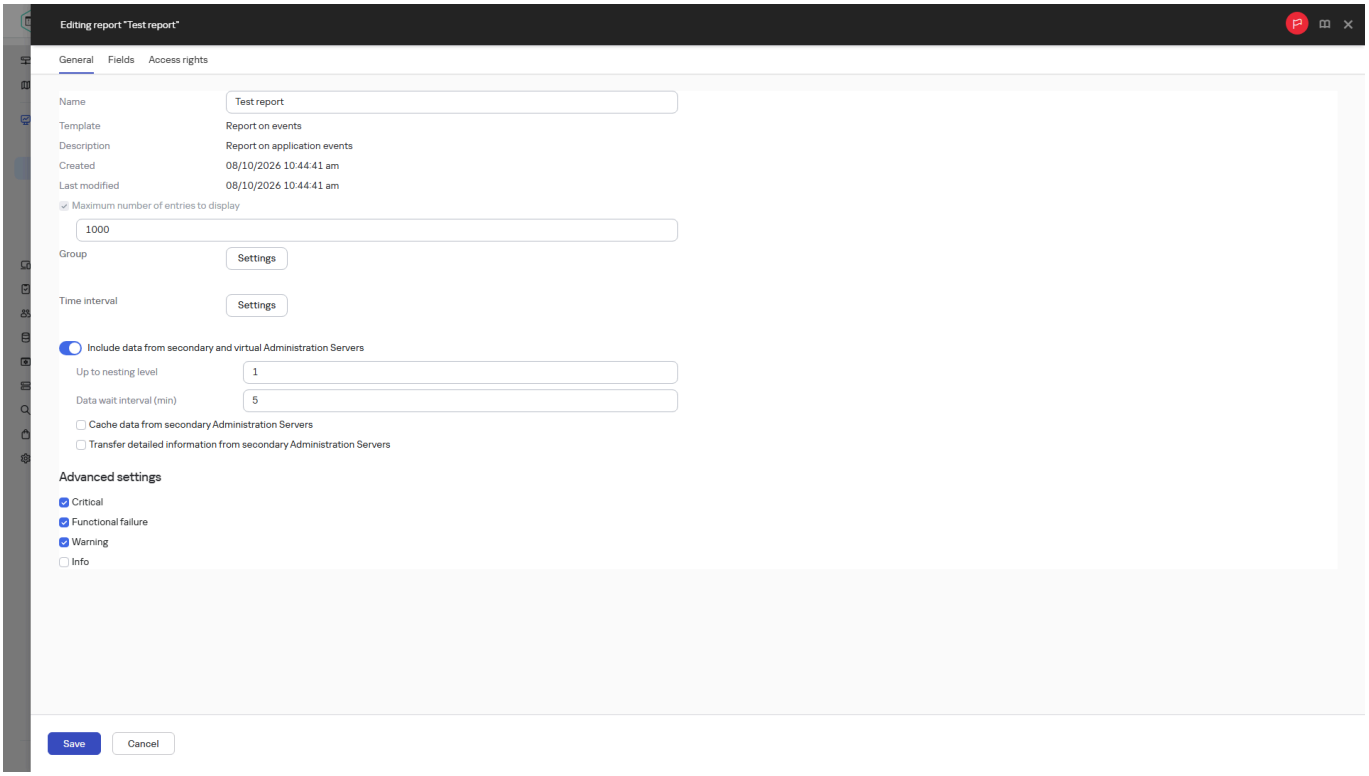
You can view and edit basic properties of a report template, for example, the report template name or the fields displayed in the report.

*To view and edit properties of a report template:*

1. In the main menu, go to **Monitoring** → **Reports**.
2. Select the check box next to the report template whose properties you want to view and edit.

   As an alternative, you can first generate the report, and then click the **Edit** button.
3. Click the **Open report template properties** button.

The **Editing report <Report name>** window opens with the **General** tab selected.




The report template properties

4. Edit the report template properties:

- **General** tab:
  - Report template name
  - **Maximum number of entries to display**

    If this option is enabled, the number of entries displayed in the table with detailed report data does not exceed the specified value. Note that this option does not affect the maximum number of events that you can include in the report when you export the report to a file.

    Report entries are first sorted according to the rules specified in the **Fields** → **Details fields** section of the report template properties, and then only the first of the resulting entries are kept. The heading of the table with detailed report data shows the displayed number of entries and the total available number of entries that match other report template settings.

    If this option is disabled, the table with detailed report data displays all available entries. We do not recommend that you disable this option. Limiting the number of displayed report entries reduces the load on the database management system (DBMS) and reduces the time required for generating and exporting the report. Some of the reports contain too many entries. If this is the case, you may find it difficult to read and analyze them all. Also, the device may run out of memory while generating such a report. This may prevent you from viewing the report.

    By default, this option is enabled. The default value is 1000.

  - **Group**

    Click the **Settings** button to change the set of client devices for which the report is created. For some types of the reports, the button may be unavailable. The actual settings depend on the settings specified during creation of the report template.

  - **Time interval**

Click the **Settings** button to modify the report period. For some types of the reports, the button may be unavailable. Available values:

- Between the two specified dates
- From the specified date to the report creation date
- From the report creation date, minus the specified number of days, to the report creation date

- **Include data from secondary and virtual Administration Servers**

  If this option is enabled, the report includes the information from the secondary and virtual Administration Servers that are subordinate to the Administration Server for which the report template is created.

  Disable this option if you want to view data only from the current Administration Server.

  By default, the option is enabled.

- **Up to nesting level**

  The report includes data from secondary and virtual Administration Servers that are located under the current Administration Server on a nesting level that is less than or equal to the specified value.

  The default value is 1. You may want to change this value if you have to retrieve information from secondary Administration Servers located at lower levels in the tree.

- **Data wait interval (min)**

  Before generating the report, the Administration Server for which the report template is created waits for data from secondary Administration Servers during the specified number of minutes. If no data is received from a secondary Administration Server at the end of this period, the report runs anyway. Instead of the actual data, the report shows data taken from the cache (if the **Cache data from secondary Administration Servers** option is enabled), or **N/A** (not available) otherwise.

  The default value is 5 minutes.

- **Cache data from secondary Administration Servers**

  Secondary Administration Servers regularly transfer data to the Administration Server for which the report template is created. There, the transferred data is stored in the cache.

  If the current Administration Server cannot receive data from a secondary Administration Server while generating the report, the report shows data taken from the cache. The date when the data was transferred to the cache is also displayed.

  Enabling this option allows you to view the information from secondary Administration Servers even if the up-to-date data cannot be retrieved. However, the displayed data can be obsolete.

  By default, this option is disabled.

- **Cache update frequency (h)**

  Secondary Administration Servers regularly transfer data to the Administration Server for which the report template is created. You can specify this period in hours. If you specify 0 hours, data is transferred only when the report is generated.

  The default value is 0.

- **Transfer detailed information from secondary Administration Servers**

  In the generated report, the table with detailed report data includes data from secondary Administration Servers of the Administration Server for which the report template is created.

Enabling this option slows the report generation and increases traffic between Administration Servers. However, you can view all data in one report.

Instead of enabling this option, you may want to analyze detailed report data to detect a faulty secondary Administration Server, and then generate the same report only for that faulty Administration Server.

By default this option is disabled.

- **Fields** tab

  Select the fields that you want to be displayed in the report. Use the **Move up** and **Move down** buttons to change the display order of fields. Use the **Add** button or **Edit** button to specify whether the information in the report must be sorted and filtered by each of the fields.

  In the **Filters of Details fields** section, you can also click the **Convert filters** button to start using the extended filtering format. This format enables you to combine filtering conditions specified in various fields by using the logical OR operation. After you click the button, the **Convert filters** panel opens on the right. Click the **Convert filters** button to confirm conversion. You can now define a converted filter with conditions from the **Details fields** section that are applied by using the logical OR operation.

  Conversion of a report to the format supporting complex filtering conditions will make the report incompatible with the previous versions of Kaspersky Security Center (11 and earlier). Also, the converted report will not contain any data from secondary Administration Servers running such incompatible versions.

5. Click **Save** to save the changes.
6. Close the **Editing report <Report name>** window.

The updated report template appears in the list of report templates.

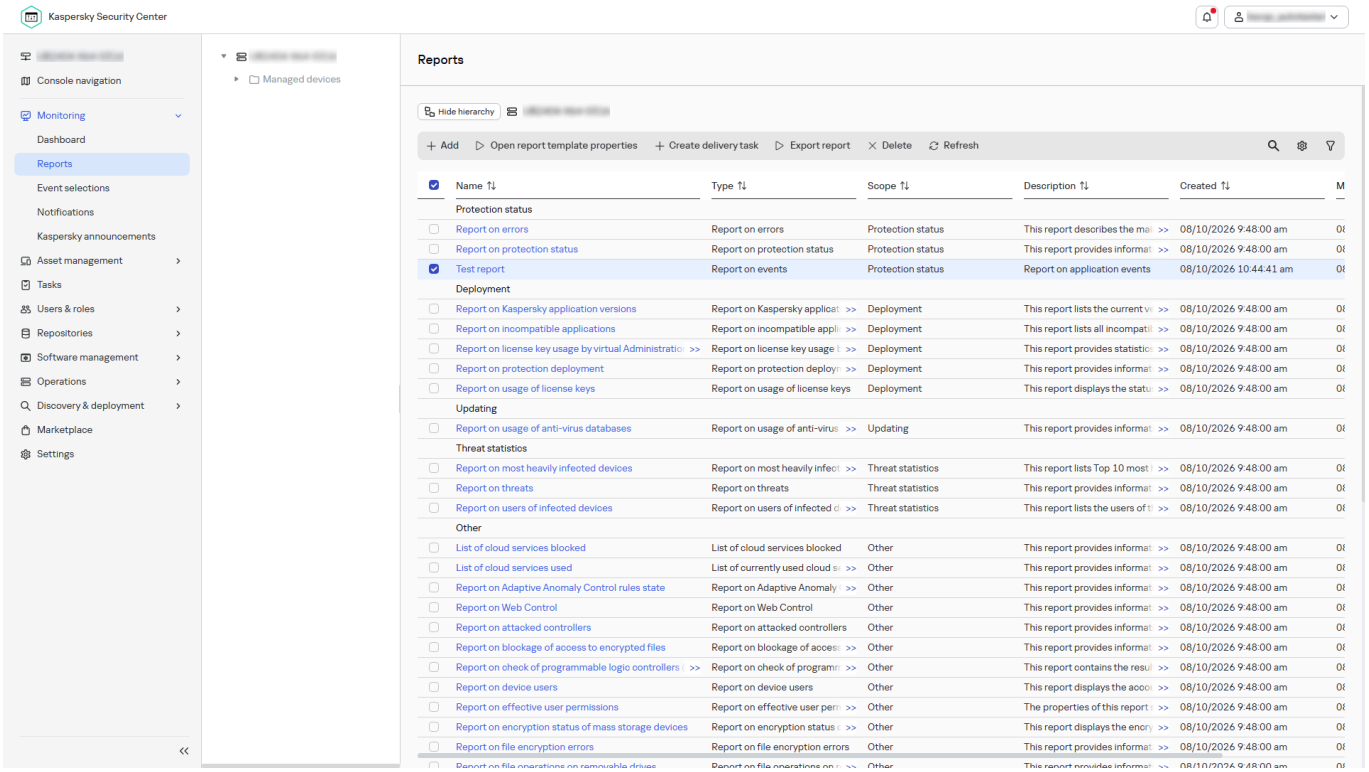
# Exporting a report to a file

You can save one or multiple reports as XML, HTML, or PDF. Kaspersky Security Center Linux allows you to export up to 10 reports to files of the specified format at the same time.

*To export a report to a file:*

1. In the main menu, go to **Monitoring** → **Reports**.
2. Choose the reports that you want to export.

If you choose more than 10 reports, the **Export report** button will be disabled.




The list of reports

3. Click the **Export report** button.

4. In the window that opens, specify the following export parameters:

   - **File name**.

     If you select one report to export, specify the report file name.

     If you select more than one report, the report file names will coincide with the name of the selected report templates.

   - **Maximum number of entries**.

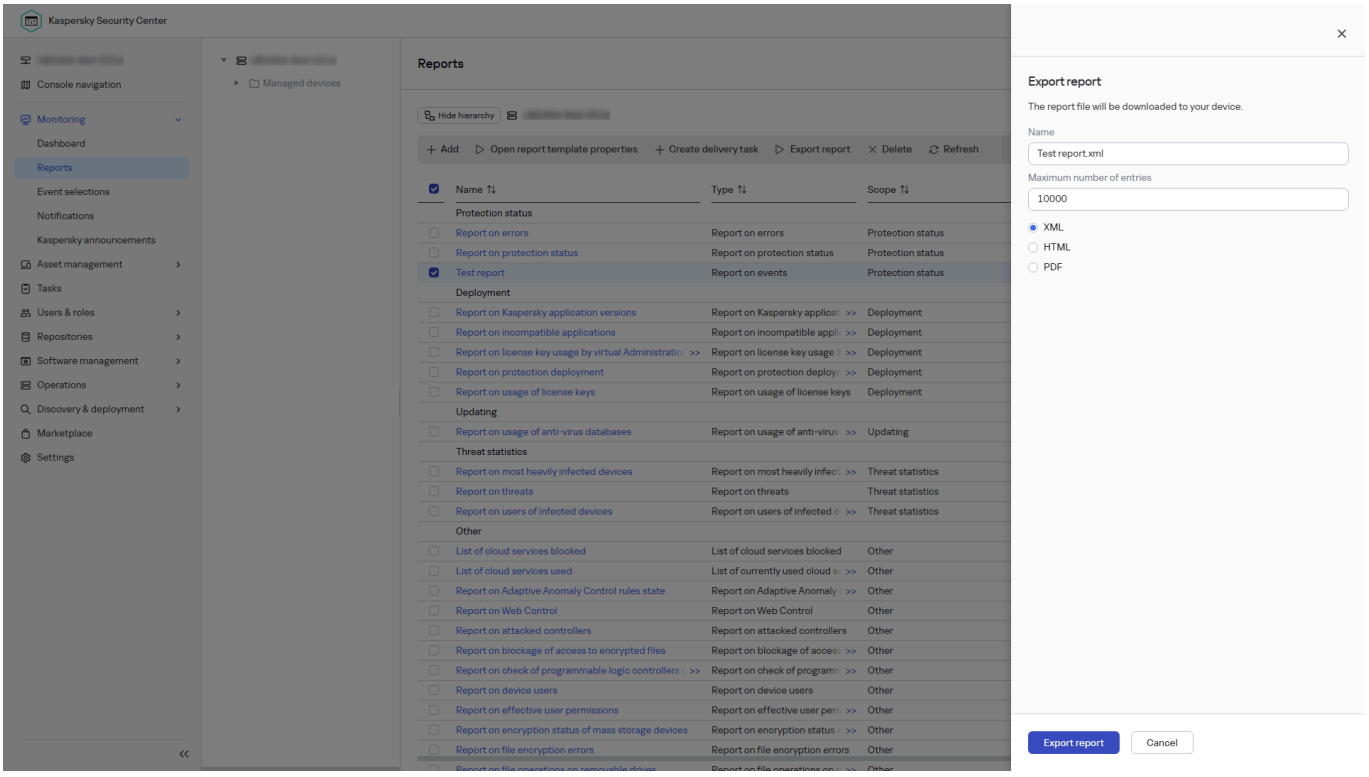
     Specify the maximum number of entries included in the report file. The default value is 10,000.

     You can export a report with an unlimited number of entries. Note that if your report contains a large number of entries, the time required for generating and exporting the report increases.

   - **File format**.

     Select the report file format: XML, HTML, or PDF. If you export multiple reports, all selected reports are saved in the specified format as separate files.

The wkhtmltopdf tool is required to convert a report to PDF. When you select the PDF option, Administration Server checks whether the wkhtmltopdf tool is installed on the device. If the tool is not installed, the application displays a message about the necessity to install the tool on the Administration Server device. Install the tool manually, and then proceed to the next step.




Specifying the report export settings

5. Click the **Export report** button.

The report is saved to a file in the specified format.

# Generating and viewing a report

*To create and view a report:*

1. In the main menu, go to **Monitoring** → **Reports**.
2. Click the name of the report template that you want to use to create a report.

   A report using the selected template is generated and displayed.

Report data is displayed according to the localization set for the Administration Server.

In the generated reports, some fonts may be displayed incorrectly on the diagrams. To resolve this issue, install the fontconfig library. Also, please check that the fonts corresponding to your operating system locale are installed in the operating system.

The report displays the following data:

- On the **Summary** tab:
  - The name and type of report, a brief description and the reporting period, as well as information about the group of devices for which the report is generated.
  - Graph chart showing the most representative report data.
  - Consolidated table with calculated report indicators.
- On the **Details** tab, a table with detailed report data is displayed.

# Creating a report delivery task

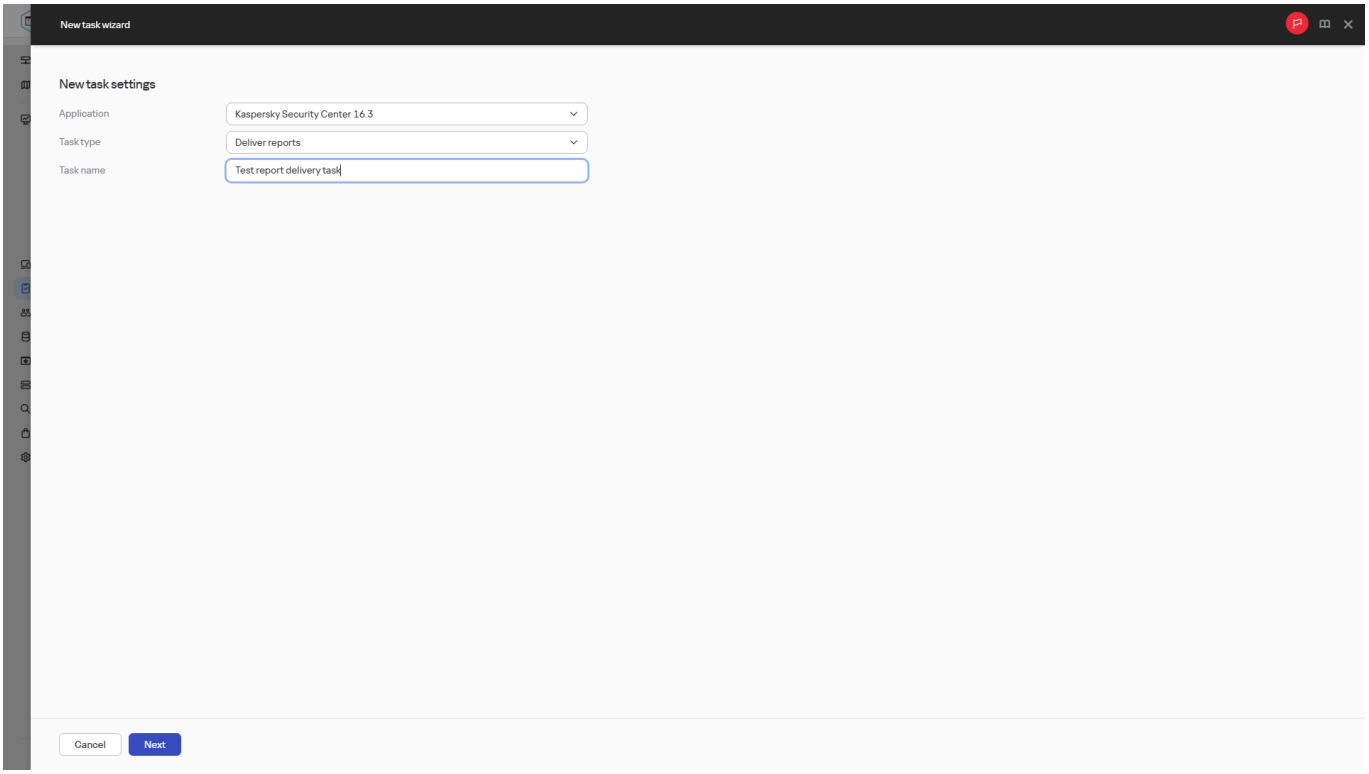
You can create a task that will deliver selected reports.

*To create a report delivery task:*

1. In the main menu, go to **Monitoring** → **Reports**.
2. Select the check boxes next to the report templates for which you want to create a report delivery task.
3. Click the **Create delivery task** button.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.
4. At the **New task settings** step of the wizard, enter the task name.

   The default name is **Deliver reports.** If a task with this name already exists, a sequence number (<N>) is added to the task name.




Creating a report delivery task

5. At the **Report configuration** step of the wizard, specify the following settings:

   a. Report templates to be delivered by the task.

   b. The report format: HTML, XLS, or PDF.

      The wkhtmltopdf tool is required to convert a report to PDF. When you select the PDF option, Administration Server checks whether the wkhtmltopdf tool is installed on the device. If the tool is not installed, the application displays a message about the necessity to install the tool on the Administration Server device. Install the tool manually, and then proceed to the next step.

   c. Whether the reports are to be sent by email, together with email notification settings.

      You can specify up to 20 email addresses. To separate email addresses, press **Enter**. You can also paste a comma-separated list of email addresses, and then press **Enter**.

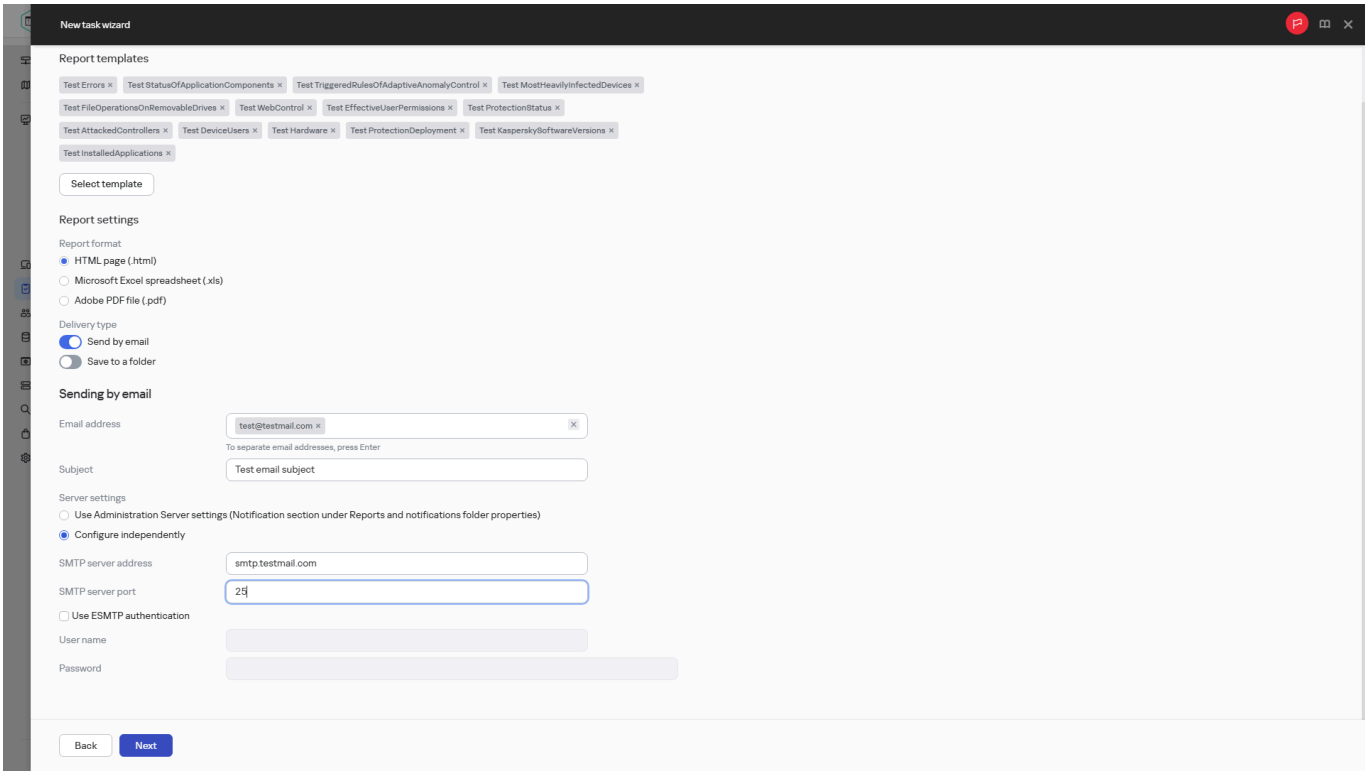
   d. Whether the reports are to be saved to a folder, together with the corresponding settings.

      After you enable the **Save to a folder** option, you must specify a POSIX path to the folder. If you want to save the reports to a shared folder, you also have to select the **Specify account for access to shared folder** check box, and then specify the user account and password for accessing this folder.

      > If you select to save the reports to a shared folder, you have to ensure the access to this folder from the device with Administration Server installed. The ways to ensure the access and the tools used depend on your infrastructure.

      When saving the reports to a local folder, credentials are usually not needed since the account under which the Administration Server is running has the access to this folder. If necessary, you can specify the user credentials at the **Selecting an account to run the task** step of the wizard.

      Regardless of the folder choice, you can also select the **Overwrite older reports of the same type** check box if you want the new report file to overwrite the file that was saved in the reports folder at the previous task startup.




Specifying the task settings

6. At the **Configure task schedule** step of the wizard, select the task start schedule.

   The following task schedule options are available:

   - **Manually**

     The task does not run automatically. You can only start it manually.

     By default, this option is selected.

   - **Every N minutes**

     The task runs regularly, with the specified interval in minutes, starting from the specified time on the day that the task is created.

     By default, the task runs every 30 minutes, starting from the current system time.

   - **Every N hours**

     The task runs regularly, with the specified interval in hours, starting from the specified date and time.

     By default, the task runs every 6 hours, starting from the current system date and time.

   - **Every N days**

     The task runs regularly, with the specified interval in days. Additionally, you can specify a date and time of the first task run. These additional options become available, if they are supported by the application for which you create the task.

     By default, the task runs every day, starting from the current system date and time.

   - **Every N weeks**

     The task runs regularly, with the specified interval in weeks, on the specified day of week and at the specified time.

     By default, the task runs every Friday at the current system time.

   - **Monthly**

     The task runs regularly, on the specified day of the month, at the specified time.

     In months that lack the specified day, the task runs on the last day.

     By default, the task runs on the first day of each month, at the current system time.

   - **On specified days**

     The task runs regularly, on the specified days of each month, at the specified time.

     By default, the start time is 18:00, and no days of the month are selected.

     > Note that you select neither a specific date in the month, nor the number of the week (first, second week of the month) but the sequence number of the weekday within a month. For example, if you set the cursor in the **Tu** cell of the **First** row, it means the task will run every first Tuesday of each new month.

     You can select several days of week.

- **On virus outbreak**

  The task runs after a *Virus outbreak* event occurs. Select application types that will monitor virus outbreaks. The following application types are available:

  - Anti-virus for workstations and file servers
  - Anti-virus for perimeter defense
  - Anti-virus for mail systems

  By default, all application types are selected.

  You may want to run different tasks depending on the security application type that reports a virus outbreak. In this case, remove the selection of the application types that you do not need.

- **On completing another task**

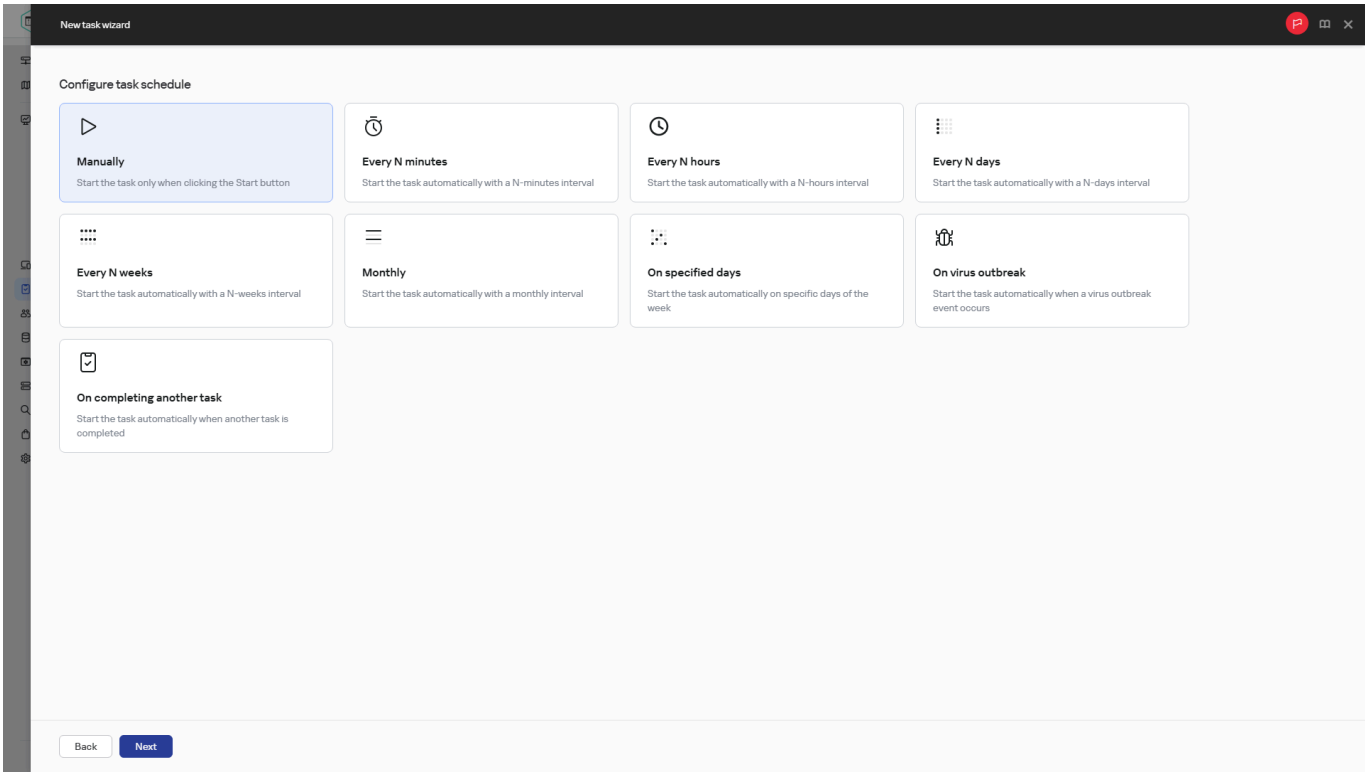
  The current task starts after another task completes. This option only works if both tasks are assigned to the same devices. For example, you may want to run the *Manage devices* task with the **Turn on the device** option and, after it completes, run the *Virus scan* task as a triggering task.

  You have to select the triggering task from the table and the status with which this task must complete (**Completed successfully** or **Failed**).

  If necessary, you can search, sort, and filter the tasks in the table as follows:

  - Enter the task name in the search field, to search the task by its name.
  - Click the sort icon to sort the tasks by name.

    By default, the tasks are sorted in alphabetical ascending order.
  - Click the filter icon, and in the window that opens, filter the tasks by group, and then click the **Apply** button.




Selecting the task start schedule

7. At this step of the wizard, configure other task schedule settings:

- In the **Task schedule** section, check or reconfigure the previously selected schedule and set the time interval, days of the month or week, set the virus outbreak condition or completing another task as a trigger to start the task. A start time can also be specified in this section if an applicable schedule is selected.

- In the **Additional settings** section, specify the following settings:

  - **Run missed tasks**

    This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

    If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

    If this option is disabled, only scheduled tasks run on client devices. For **Manually**, **Once** and **Immediately** schedule, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

    By default, this option is enabled.

  - **Use automatically randomized delay for task starts**

    If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

    The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However, when task settings are edited or the task is started manually, the calculated value of the task start time changes.

    If this option is disabled, the task starts on client devices according to the schedule.

    By default, this option is enabled.

  - **Use automatically randomized delay for task starts within an interval of**

    If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

    If this option is disabled, the task starts on client devices according to the schedule.

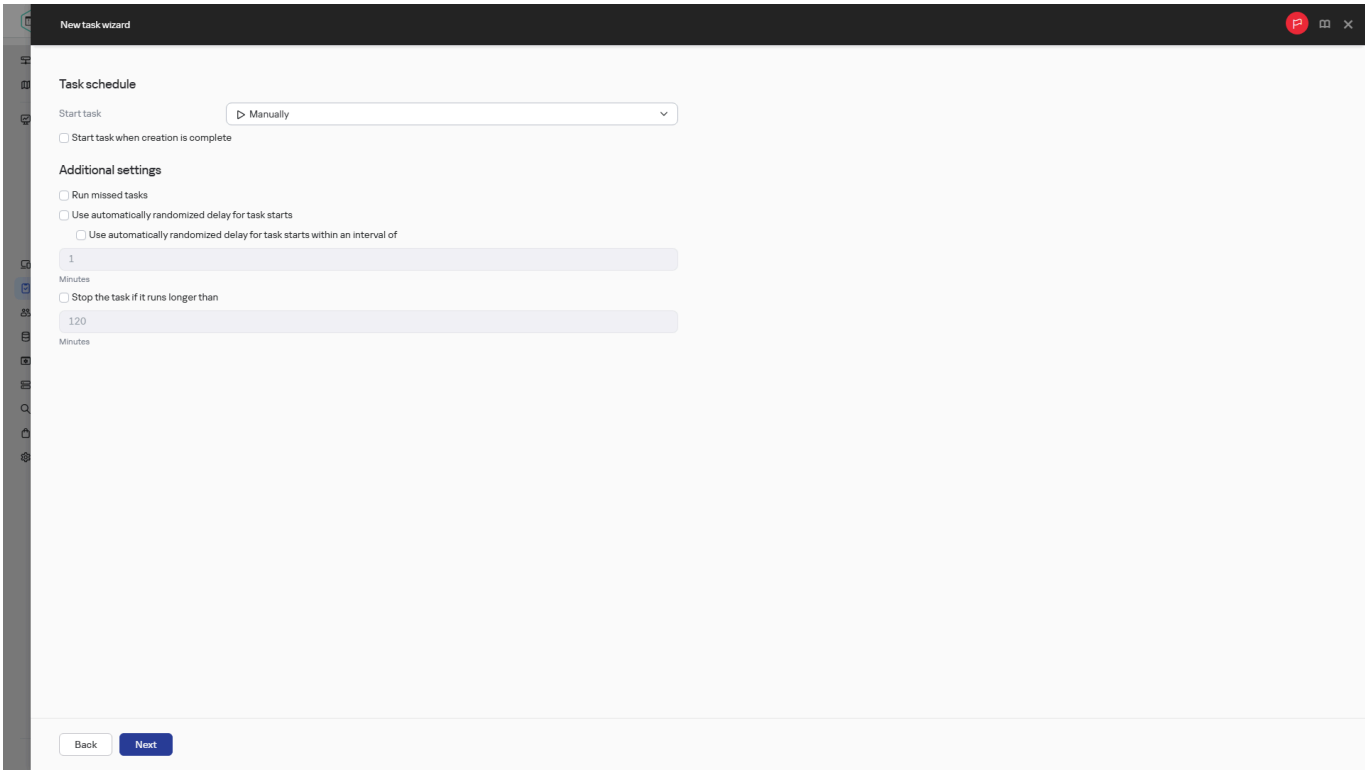
    By default, this option is disabled. The default time interval is one minute.

  - **Stop the task if it runs longer than**

    After the specified time period expires, the task is stopped automatically, whether it is completed or not.

    Enable this option if you want to interrupt (or stop) tasks that take too long to execute.

By default, this option is disabled. The default task execution time is 120 minutes.

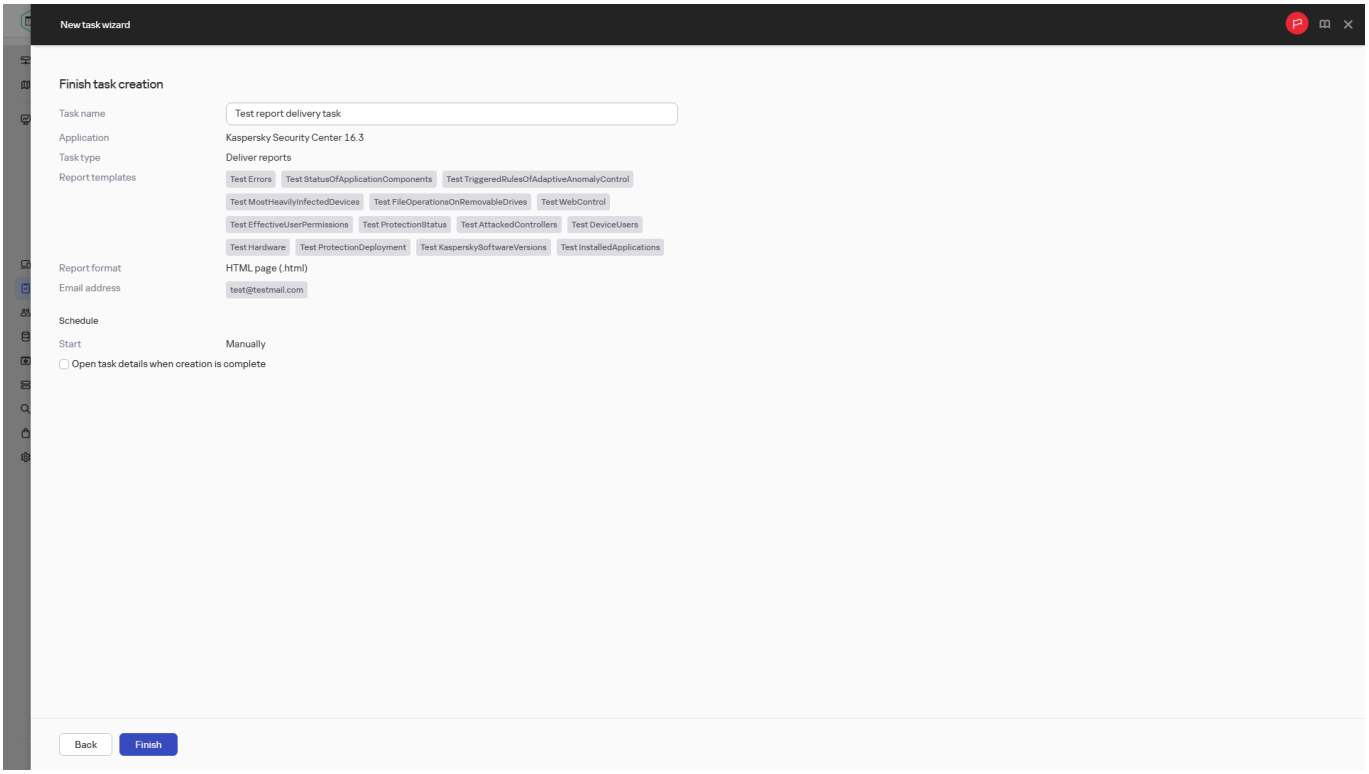



Specifying the task schedule settings

8. At the **Selecting an account to run the task** step of the wizard, specify the credentials of the user account that is used to run the task.

9. If you want to modify other task settings after the task is created, at the **Finish task creation** step of the wizard, enable the **Open task details when creation is complete** option. By default, the option is enabled.

10. Click the **Finish** button to create the task and close the wizard.




Finishing task creation

The report delivery task is created. If the **Open task details when creation is complete** option is enabled, the

task settings window opens.

# Deleting report templates

*To delete one or several report templates:*

1. In the main menu, go to the **Monitoring** → **Reports**.
2. Select check boxes next to the report templates that you want to delete.
3. Next, click the **Delete** button.
4. In the window that opens, click **OK** to confirm your selection.

The selected report templates are deleted. If these report templates were included in the report delivery tasks, they are also removed from the tasks.

# Hardening center

The Hardening center displays up-to-date information about the protection of the Administration Server and distribution points. This information is presented as protection level indicators. These indicators allow tracking the implementation of the Hardening Guide, as well as promptly address security issues in your infrastructure as they arise.

The indicator can be in one of the following statuses:

- Protection configured.
- Protection partially configured.
- Protection not configured.

## How to view detailed information about the protection level

The overall indicator status is formed by the states of protection parameters.

*To open the **Hardening center**:*

1. In the main menu, go to the **Monitoring** → **Dashboard** section.
2. Click the protection status in the upper-right corner.

In the **Hardening center** window that opens, the parameters are grouped by protected objects: Administration server and distribution points.

Each protection parameter is displayed in one of the states depending on your access rights:

- ✅ if there are no issues to resolve or you do not have the required access rights.
- ⚠️ or ❌ if there are issues to be resolved.

The following parameters are displayed for Administration Server only:

- Backup configured
- Administration Server maintenance configured
- TLS encryption enabled

The following parameters are displayed both for Administration Server and distribution points:

- Security application installed
- Security application policy applied
- Anti-virus database updates configured
- All devices are managed

  This setting is also displayed for devices that are not distribution points or Administration Server devices.

**Special considerations for Administration Server:**

- All protection parameters are calculated for physical administration server only and not applied to virtual servers.

  If you have a hierarchical structure of several Administration Servers, the protection level indicator is calculated for each physical server separately.

- The **Security application installed**, **Security application policy applied**, **Anti-virus database updates configured** are calculated for a device with Administration Server installed.

- When deploying a Kaspersky Security Center Linux failover cluster, the **Security application installed**, **Security application policy applied, Anti-virus database updates configured** and **All devices are managed** parameters are evaluated for each node. The node is considered in the indicator status calculation only after it becomes active.

## How the indicator status is calculated

The table below describes how the indicator status is evaluated.

| Indicator status | Condition |
| --- | --- |
| Protection configured. | All protection parameters are in ✅ state. |

| | |
|---|---|
| Protection partially configured. | The **Anti-virus database updates configured** parameter is in the ⚠ state, while all other parameters are in the ✓ state. |
| Protection not configured. | If at least one of the following protection parameter is in ✗ state. |

# Security application installed

Security applications allow you to protect your devices against various types of threats, including network, phishing, and scam attacks.

The parameter is displayed in ✓ state if one of the conditions is met:

- You have no access rights to the devices.
- You have the **Read** right in the **General features** → **Basic functionality** functional area, while Network Agent and a security application are installed on the devices.

  The condition must be met on all the devices available to you based on your access rights, excluding the devices with an installed application that does not require any anti-virus protection (for example, a secured operating system), devices with no Network Agent installed so the information about the device appeared on Administration Server less than 24 hours ago, and the offline devices that were last connected to Administration Server 7 or more days ago.

The parameter is displayed in ✗ state if at least one of the conditions below is met.

You have to click the **View devices** button, and perform the actions described in the table for the displayed devices.

| Condition | Solution |
|---|---|
| Network Agent is not installed on the device | Install Network Agent.<br>For the Administration Server device, the simplest way of Network Agent installation is to use a stand-alone installation package. |
| The device is included in the **Unassigned devices** group | Move the device to the Managed devices group or its subgroup |
| No security applications were found, or real-time protection is not running for the installed security application | Install a security application. The application will transmit data about protection state to Administration Server.<br>You can view protection status of a device in the device settings: **General** section → **Device status**.<br>On the Administration Server device, you must install Kaspersky Endpoint Security for Linux. |

# Policy applied

A policy is a set of security application settings that are applied to an administration group and its subgroups.

The parameter is displayed in ✅ state if one of the conditions is met:

- You have no access rights to the devices.
- You have the **Read** right in the **General features → Basic functionality** functional area, while a security application is installed on your devices, and an active policy of this security application is applied to the devices.

> The condition must be met on all the devices available to you based on your access rights, excluding the devices with an installed application that does not require any anti-virus protection (for example, a secured operating system), devices with no Network Agent installed so the information about the device appeared on Administration Server less than 24 hours ago, and the offline devices that were last connected to Administration Server 7 or more days ago.

The parameter is displayed in ❌ state if at least one of the conditions below is met.

You have to click the **View devices** button, and perform the actions described in the table for the displayed devices.

| Condition | Solution |
|---|---|
| Security application is not installed on the device. | Make sure that the device is absent in the selection for the **Security application installed** protection parameter. |
| A policy is not applied to the device. | Make sure that the policy is created for the administration group to which the device belongs.<br>If not, create and activate the policy.<br>If yes, make sure that:<br>• The created policy is active. If not, activate the policy.<br>• The policy distribution status is **Applied successfully**.<br>If the status is **Applied with error**, the issue must be fixed on the security application side. |

# Anti-virus databases update configured

Since Anti-virus databases protect your devices from threats, you have to update databases on the devices in a regular and timely manner.

The parameter is displayed in ✅ state if one of the conditions is met:

- You have no access rights to the devices.
- You have the Read right in the General features → Basic functionality functional area, and the anti-virus databases are updated on the devices.

> The condition must be met on all the devices available to you based on your access rights, excluding the devices with an installed application that does not require any anti-virus protection (for example, a secured operating system), devices with no Network Agent installed so the information about the device appeared on Administration Server less than 24 hours ago, and the offline devices that were last connected to Administration Server 7 or more days ago.

The parameter is displayed in ⚠️ state if anti-virus databases were last updated on a device more than 3 days ago.

The parameter is displayed in ❌ state if anti-virus databases were last updated on a device more than 7 days ago.

*To resolve the issue:*

1. Click the View devices button next to the parameter.
2. For the devices that are displayed, perform the following actions:
   a. Make sure that connection between Network Agent and Administration Server is established.
      If not, refer to the following articles:
      Troubleshooting the problems with updating anti-virus databases of Kaspersky Endpoint Security for Linux
      Problems when updating anti-virus databases from the Kaspersky Security Center repository
   b. Make sure that the Kaspersky application whose anti-virus databases you are checking is not stopped.
      If the application is stopped, start it.
   c. On the device, view the errors that occurred after update.

# Backup configured

For recommendations on Administration Server data backup, refer to Backup copying and restoration of Administration Server data.

The parameter is displayed in state if one of the conditions is met:

- You have no access rights to work with the Administration Server data backup task.
- You have the **Read, Write**, and **Execute** rights in the **General features** → **Operations on Administration Server** functional area, and backup is configured and performed on a regular basis.

The parameter is displayed in state if at least one of the conditions below is met.

| Condition | Solution |
|---|---|
| The Administration Server data backup task is not created. | Create the task. |
| Necessary schedule settings are not configured for the Administration Server data backup task. | In the Administration Server maintenance task, specify the **Start task** settings other than **On virus outbreak** and **Manually**. |

# Administration Server maintenance configured

The Administration Server maintenance allows you to free up space in the folder of the Administration Server as well as to minimize the database size. This helps to accelerate request processing and increases the overall stability of the system.

The parameter is displayed in ✅ state if one of the conditions is met:

- You have no access rights to work with the Administration Server maintenance task.
- You have the **Read, Write**, and **Execute** rights in the **General features → Operations on Administration Server** functional area, while Administration Server maintenance configured and performed on a regular basis.

  The rights must be set at the Administration Server level.

The parameter is displayed in ❌ state if at least one of the conditions below is met.

| Condition | Solution |
|---|---|
| Administration Server maintenance task is not created. | Create the task. |
| Necessary schedule settings are not configured for the Administration Server maintenance task. | In the Administration Server maintenance task, specify the **Start task** settings other than **On virus outbreak** and **Manually**. |

# TLS encryption enabled

You must ensure that only 1.2 and 1.3 versions of TLS protocol are allowed. Allowing earlier versions results in serious data security risks and makes systems vulnerable to attacks.

The parameter is displayed in ✅ state if only 1.2 and 1.3 version of TLS protocol are allowed.

The parameter is displayed in ❌ state if outdated TLS versions earlier than 1.2 are allowed.

To resolve the issue, you have to set the `SrvUseStrictSslSettings` flag to `4` or `5` value.

# All devices are managed

You can use this parameter to identify devices that are potentially out of control.

For the Administration Server to be able to detect managed devices during a network scan, you need to configure regular polling of IP ranges or polling of the Windows network. Set the polling period to no more than three total Network Agent synchronization periods, taking into account the time spent on processing the polled data.

Devices that have a shorter synchronization period may erroneously affect the state of the indicator.

In the following table, you can find calculations of polling intervals for selected synchronization periods.

| Synchronization interval (min) | Number of managed devices | Maximum IP and Windows network polling intervals (min) |
|---|---|---|
| 15 | 10,000 | 35 |
| 30 | 20,000 | 80 |
| 45 | 30,000 | 120 |

| | | |
|---|---|---|
| 60 | 40,000 | 165 |
| 75 | 50,000 | 210 |

Re-evaluation of the status may take some time.

This parameter is displayed with the status when one of the following conditions is satisfied:

- You have no access rights to the devices.
- You have the **Read** permission in **General features** → **Basic functionality** functional area, the devices are in the **Managed devices** group, and a connection has been established between Administration Server and Network Agent on the devices.

  This condition must be satisfied on all devices available to you in accordance with your access rights, except for: devices whose information appeared on Administration Server less than 24 hours ago, and devices that last connected to Administration Server seven or more days ago.

This parameter is displayed with the status if there is at least one device for which one of the conditions below is satisfied.

You have to click the **View devices** button, and perform the actions described in the table for the displayed devices.

| Condition | Solution |
|---|---|
| Network Agent is not installed on a device included in the **Managed devices** group. | Install Network Agent. |
| Administration Server detects a managed device during a network scan, but this devices has not connected to Administration Server for three synchronization intervals in a row. | Do the following:<br>1. Run the klnagchk utility on the problematic device to see if the service is running and Network Agent can connect to Administration Server.<br>2. Check the network accessibility of Administration Server and connection gateways.<br>3. Restore the connection of the device to Administration Server by using the klmover utility.<br>4. Remove obsolete devices from administration groups.<br><br>If your infrastructure has managed devices that continue to respond to network polls when powered off, such devices may erroneously affect the state of the indicator.<br>You can do the following actions with problematic devices:<br>a. Verify that the device is managed by Administration Server.<br>b. Move this device to a separate administration group.<br>c. In this administration group, set the **Device has become unmanaged** condition to any status other than *Critical*. |

# Events and event selections

This section provides information about events and event selections, about the types of events that occur in Kaspersky Security Center Linux components, and about managing frequent events blocking.

# About events in Kaspersky Security Center Linux

Kaspersky Security Center Linux allows you to receive information about events that occur during the operation of Administration Server and Kaspersky applications installed on managed devices. Information about events is saved in the Administration Server database.

## Events by type

In Kaspersky Security Center Linux, there are the following types of events:

- General events. These events occur in all managed Kaspersky applications. An example of a general event is Virus outbreak. General events have strictly defined syntax and semantics. General events are used, for instance, in reports and dashboards.
- Managed Kaspersky applications-specific events. Each managed Kaspersky application has its own set of events.

## Events by source

You can view the full list of the events that can be generated by an application on the **Event configuration** tab in the application policy. For Administration Server, you can additionally view the event list in the Administration Server properties.

Events can be generated by the following applications:

- Kaspersky Security Center Linux components:
  - Administration Server
  - Network Agent
- Managed Kaspersky applications

  For details about the events generated by Kaspersky managed applications, please refer to the documentation of the corresponding application.

Events by importance level

Each event has its own importance level. Depending on the conditions of its occurrence, an event can be assigned various importance levels. There are four importance levels of events:

- A *critical event* is an event that indicates the occurrence of a critical problem that may lead to data loss, an operational malfunction, or a critical error.
- A *functional failure* is an event that indicates the occurrence of a serious problem, error, or malfunction that occurred during operation of the application or while performing a procedure.
- A *warning* is an event that is not necessarily serious, but nevertheless indicates a potential problem in the future. Most events are designated as warnings if the application can be restored without loss of data or functional capabilities after such events occur.
- An *info* event is an event that occurs for the purpose of informing about successful completion of an operation, proper functioning of the application, or completion of a procedure.

Each event has a defined storage term, during which you can view or modify it in Kaspersky Security Center Linux. Some events are not saved in the Administration Server database by default because their defined storage term is zero. Only events that will be stored in the Administration Server database for at least one day can be exported to external systems.

# Events of Kaspersky Security Center Linux components

Each Kaspersky Security Center Linux component has its own set of event types. This section lists types of events that occur in Administration Server and Network Agent. Types of events that occur in Kaspersky applications are not listed in this section.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. For Administration Server, you can additionally view and configure the event list in the Administration Server properties. If you want to configure notification settings for all the events at once, configure general notification settings in the Administration Server properties.

## Data structure of event type description

For each event type, its display name, identifier (ID), alphabetic code, description, and the default storage term are provided.

- **Event type display name**. This text is displayed in Kaspersky Security Center Linux when you configure events and when they occur.
- **Event type ID**. This numerical code is used when you process events by using third-party tools for event analysis.
- **Event type** (alphabetic code). This code is used when you browse and process events by using public views that are provided in the Kaspersky Security Center Linux database and when events are exported to a SIEM system.

- **Description**. This text contains the situations when an event occurs and what you can do in such a case.
- **Default storage term**. This is the number of days during which the event is stored in the Administration Server database and is displayed in the list of events on Administration Server. After this period elapses, the event is deleted. If the event storage term value is 0, such events are detected but are not displayed in the list of events on Administration Server. If you configured to save such events to the operating system event log, you can find them there.

  You can change the storage term for events: Setting the storage term for an event.

# Administration Server events

This section contains information about the events related to the Administration Server.

## Administration Server critical events

The table below shows events of Administration Server that have the **Critical** severity.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. For Administration Server, you can additionally view and configure the event list in the Administration Server properties. If you want to configure notification settings for all the events at once, configure general notification settings in the Administration Server properties.

Administration Server critical events

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Administration Server certificate for mobile devices has expired** | 6129 | KLSRV_EV_SRV_CERT_EXPIRED_DN | Events of this type occur when the Administration Server certificates for mobile devices and UEFI devices expires.<br>You need to update the expired certificate. | 180 days |
| **Audit: Export to SIEM failed** | 5130 | KLAUD_EV_SIEM_EXPORT_ERROR | Events of this type occur when exporting events to the SIEM system failed due to a connection error with the SIEM system. | 180 days |
| **Device has become unmanaged** | 4111 | KLSRV_HOST_OUT_CONTROL | Events of this type occur if a managed device is visible on the network but has not connected to Administration Server for a specific period.<br>Find out what prevents the proper functioning of Network Agent on the device. Possible causes include network issues and removal of Network Agent from the device. | 180 days |
| **Device status is Critical** | 4113 | KLSRV_HOST_STATUS_CRITICAL | Events of this type occur when a managed device is assigned the *Critical* status. You can configure the conditions under which the device status is changed to *Critical*. | 180 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **License expires soon** | 4129 | KLSRV_EV_LICENSE_SRV_EXPIRE_SOON | Events of this type occur when the commercial license expiration date is approaching.<br>Once a day Kaspersky Security Center Linux checks whether a license expiration date is approaching. Events of this type are published 30 days, 15 days, 5 days, and 1 day before the license expiration date. This number of days cannot be changed. If the Administration Server is turned off on the specified day before the license expiration date, the event will not be published until the next day.<br>When the commercial license expires, Kaspersky Security Center Linux provides only basic functionality.<br>You can respond to the event in the following ways:<br>• Make sure that a reserve license key is added to Administration Server.<br>• If you use a subscription, make sure to renew it. An unlimited subscription is renewed automatically if it has been prepaid to the service provider by the due date. | 180 days |
| **License limit has been exceeded** | 4099 | KLSRV_EV_LICENSE_CHECK_MORE_110 | Once a day Kaspersky Security Center Linux checks whether a licensing limit is exceeded.<br>Events of this type occur when Administration Server detects that some license limits are exceeded by Kaspersky applications installed on client devices and if the number of currently used licensing units covered by a single license exceeds 110% of the total number of units covered by the license.<br>Even when this event occurs, client devices are protected.<br>You can respond to the event in the following ways:<br>• Look through the managed devices list. Delete devices that are not in use.<br>• Provide a license for more devices (add a valid activation code or a key file to Administration Server).<br>Kaspersky Security Center Linux determines the rules to generate events when a licensing limit is exceeded. | 180 days |
| **Limited functionality mode** | 4130 | KLSRV_EV_LICENSE_SRV_LIMITED_MODE | Events of this type occur when Kaspersky Security Center Linux starts to operate with basic functionality, without Vulnerability and patch management and without Mobile Device Management features.<br>Following are causes of, and appropriate responses to, the event:<br>• License term has expired. Provide a license to use the full functionality mode of Kaspersky Security Center Linux (add a valid activation code or a key file to Administration Server).<br>• Administration Server manages more devices than specified by the license limit. Move devices from the administration groups of an Administration Server to those of another Administration Server (if the license limit of the other Administration Server allows). | 180 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **MDM certificate has expired** | 4132 | KLSRV_CERTIFICATE_EXPIRED | Events of this type occur when the client certificate on mobile devices expires. | 180 days |
| **The key file has been added to the denylist** | 4124 | KLSRV_LICENSE_BLACKLISTED | Events of this type occur when Kaspersky has added the activation code or key file that you use to the denylist.<br>Contact Technical Support for more details. | 180 days |
| **Updates for Kaspersky application modules have been revoked** | 4142 | KLSRV_SEAMLESS_UPDATE_REVOKED | Events of this type occur if updates have been revoked by Kaspersky experts, for example, to replace them with newer versions. For such updates, the status is *Revoked*. The event concerns Kaspersky Security Center Linux patches and does not concern modules of managed Kaspersky applications. The event provides the reason that the seamless updates are not installed. | 180 days |
| **Virus outbreak** | • 26 (for File Threat Protection)<br>• 27 (for Mail Threat Protection)<br>• 28 (for firewall) | GNRL_EV_VIRUS_OUTBREAK | Events of this type occur when the number of malicious objects detected on several managed devices exceeds the threshold within a short period.<br>You can respond to the event in the following ways:<br>• Configure the threshold in the Administration Server properties.<br>• Create a stricter policy that will be activated, or create a task that will be run, at the occurrence of this event. | |

## Administration Server functional failure events

The table below shows the events of Administration Server that have the **Functional failure** importance level.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. For Administration Server, you can additionally view and configure the event list in the Administration Server properties. If you want to configure notification settings for all the events at once, configure general notification settings in the Administration Server properties.

Administration Server functional failure events

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Failed to copy the updates to the specified folder** | 4123 | KLSRV_UPD_REPL_FAIL | Events of this type occur when software updates are copied to an additional shared folder(s).<br>You can respond to the event in the following ways:<br>• Check whether the user account that is employed to gain access to the folder(s) has write permission.<br>• Check whether a user name and/or a password to the folder(s) is/are changed.<br>• Check the internet connection, as it might be the cause of the event. Follow the instructions to update databases and software modules. | 180 days |
| **Failed to poll the cloud segment** | 4143 | KLSRV_KLCLOUD_SCAN_ERROR | Events of this type occur when Administration Server fails to poll a network segment in a cloud environment. Read the details in the event description and respond accordingly. | Not stored |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Limit of installations has been exceeded for one of the licensed applications groups** | 4126 | KLSRV_INVLICPROD_EXCEDED | Administration Server generates events of this type periodically (every hour). Events of this type occur if in Kaspersky Security Center Linux you manage license keys of third-party applications and if the number of installations has exceeded the limit set by the license key of the third-party application.<br>You can respond to the event in the following ways:<br>• Look through the managed devices list. Delete the third-party application from devices on which the application is not in use.<br>• Use a third-party license for more devices.<br>You can manage license keys of third-party applications using the functionality of licensed applications groups. A licensed applications group includes third-party applications that meet criteria set by you. | 180 days |
| **No free disk space** | 4107 | KLSRV_DISK_FULL | Events of this type occur when the hard drive of the device on which Administration Server is installed runs out of free space.<br>Free up disk space on the device. | 180 days |
| **No free space in the Administration Server database** | 4110 | KLSRV_DATABASE_FULL | Events of this type occur when there is no free space in the Administration Server database.<br>Administration Server does not function when its database has reached its capacity and when further recording to the database is not possible.<br>Following are the causes of this event, depending on the DBMS that you use, and appropriate responses to the event:<br>• Limit the number of events to store in the Administration Server database.<br>• In the Administration Server database, there are too many events sent by the Application Control component. You can change the settings of the Kaspersky Endpoint Security policy relating to Application Control event storage in the Administration Server database.<br>Review the information on DBMS selection. | 180 days |
| **Runtime error** | 4125 | KLSRV_RUNTIME_ERROR | Events of this type occur because of unknown issues.<br>Most often these are DBMS issues, network issues, and other software and hardware issues.<br>Details of the event can be found in the event description. | 180 days |
| **Shared folder is not available** | 4108 | KLSRV_SHARED_FOLDER_UNAVAILABLE | Events of this type occur if the shared folder of Administration Server is not available.<br>You can respond to the event in the following ways:<br>• Check whether the Administration Server (where the shared folder is located) is turned on and available.<br>• Check whether a user name and/or a password to the folder is/are changed.<br>• Check the network connection. | 180 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **The Administration Server database is unavailable** | 4109 | KLSRV_DATABASE_UNAVAILABLE | Events of this type occur if the Administration Server database becomes unavailable.<br>You can respond to the event in the following ways:<br>• Check whether the remote server that has the DBMS installed is available.<br>• View the DBMS logs to discover the reason for Administration Server database unavailability. | 180 days |

## Administration Server warning events

The table below shows the events of Network Agent that have the **Warning** severity level.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. For Administration Server, you can additionally view and configure the event list in the Administration Server properties. If you want to configure notification settings for all the events at once, configure general notification settings in the Administration Server properties.

Administration Server warning events

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Administration Server certificate for mobile devices is expiring** | 6128 | KLSRV_EV_SRV_CERT_EXPIRES_SOON | Events of this type occur when the Administration Server certificates for mobile devices and UEFI devices expires.<br>You need to update the expired certificate. | 90 days |
| **APNs certificate expires soon** | 4136 | KLSRV_APN_CERTIFICATE_EXPIRES_SOON | Events of this type occur when there are fewer than 14 days left before the APNs certificate expires.<br>When the APNs certificate expires, you need to manually renew the APNs certificate and install it on an iOS MDM Server.<br>We recommend that you schedule the APNs certificate renewal in advance of the expiration date. | Not stored |
| **APNs certificate has expired** | 4135 | KLSRV_APN_CERTIFICATE_EXPIRED | Events of this type occur when an APNs certificate expires.<br>You need to manually renew the APNs certificate and install it on an iOS MDM Server. | Not stored |
| **Audit: Test connection to SIEM server failed** | 5120 | KLAUD_EV_SIEM_TEST_FAILED | Events of this type occur when an automatic connection test to the SIEM server failed. | 90 days |
| **Certificate has been removed** | 4134 | KLSRV_CERTIFICATE_REMOVED | Events of this type occur when an administrator removes any type of certificate (General, Mail, VPN) for Mobile Device Management.<br>After removing a certificate, mobile devices connected via this certificate will fail to connect to Administration Server.<br>This event might be helpful when investigating malfunctions associated with the management of mobile devices. | 90 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Certificate has been requested** | 4133 | KLSRV_CERTIFICATE_REQUESTED | Events of this type occur when a certificate for Mobile Device Management fails to be automatically reissued.<br>Following might be the causes and appropriate responses to the event:<br>• Automatic reissue was initiated for a certificate for which the **Reissue certificate automatically if possible** option is disabled. This might be due to an error that occurred during creation of the certificate. Manual reissue of the certificate might be required.<br>• If you use an integration with a public key infrastructure, the cause might be a missing SAM-Account-Name attribute of the account used for integration with PKI and for issuance of the certificate. Review the account properties. | 90 days |
| **Conflict of device names** | 4102 | KLSRV_EVENT_HOSTS_CONFLICT | Events of this type occur when Administration Server considers two or more managed devices as a single device.<br>Most often this happens when a cloned hard drive was used for software deployment on managed devices and without switching the Network Agent to the dedicated disk cloning mode on a reference device.<br>To avoid this issue, switch Network Agent to the disk cloning mode on a reference device before cloning the hard drive of this device. | 90 days |
| **Connection to the primary Administration Server has been interrupted** | 4118 | KLSRV_EV_MASTER_SRV_DISCONNECTED | Events of this type occur when a connection to the primary Administration Server is interrupted.<br>Read the operating system log on the device where the primary Administration Server is installed and respond accordingly. | 90 days |
| **Connection to the secondary Administration Server has been interrupted** | 4116 | KLSRV_EV_SLAVE_SRV_DISCONNECTED | Events of this type occur when a connection to the secondary Administration Server is interrupted.<br>Read the operating system log on the device where the secondary Administration Server is installed and respond accordingly. | 90 days |
| **Device has remained inactive on the network for a long time** | 4103 | KLSRV_EVENT_HOSTS_NOT_VISIBLE | Events of this type occur when a managed device shows inactivity for some time.<br>Most often, this happens when a managed device is decommissioned.<br>You can respond to the event in the following ways:<br>• Manually remove the device from the list of managed devices.<br>Specify the time interval after which the **Device has remained inactive on the network for a long time** event is created by using Kaspersky Security Center Web Console.<br>• Specify the time interval after which the device is automatically removed from the group by using Kaspersky Security Center Web Console. | 90 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Device status is Warning** | 4114 | KLSRV_HOST_STATUS_WARNING | Events of this type occur when a managed device is assigned the *Warning* status. You can configure the conditions under which the device status is changed to *Warning*. | 90 days |
| **Failed to download file to device** | 4165 | KLSRV_FILE_DOWNLOAD_FAILED | Events of this type occur in the following cases:<br>• You try to download a file to the corporate container, but a corporate container has not been created.<br>• There is not enough space on the device.<br>• Information about the file failed to download from the server.<br>• The file contents failed to download from the server.<br>• The folder could not be created on the device.<br>• The file access permission is missing on the personal device.<br>• The file access permission is missing in the corporate container. | 90 days |
| **Failed to send the FCM message to the FCM server** | 4140 | KLSRV_GCM_GENERAL_ERROR | Events of this type occur due to unexpected errors on the Administration Server side when working with the Google Firebase Cloud Messaging HTTP protocol.<br>Read the details in the event description and respond accordingly.<br>If you cannot find the solution to an issue on your own, we recommend that you contact Kaspersky Technical Support. | 90 days |
| **Failed to send the FCM message to the mobile device** | 4138 | KLSRV_GCM_DEVICE_ERROR | Events of this type occur when Mobile Device Management is configured to use Google Firebase Cloud Messaging (FCM) for connecting to managed mobile devices with an Android operating system and FCM Server fails to handle some of the requests received from Administration Server. It means that some of the managed mobile devices will not receive a push notification.<br>Read the HTTP code in the details of the event description and respond accordingly. For more information on the HTTP codes received from FCM Server and related errors, please refer to the Google Firebase service documentation (see chapter "Downstream message error response codes"). | 90 days |
| **Frequent events have been detected** | | KLSRV_EVENT_SPAM_EVENTS_DETECTED | Events of this type occur when Administration Server detects a frequent event on a managed device. Refer to the following section for details: Blocking frequent events. | 90 days |
| **Hard drive almost full** | 4105 | KLSRV_NO_SPACE_ON_VOLUMES | Events of this type occur when the hard drive of the device on which Administration Server is installed almost runs out of free space.<br>Free up disk space on the device. | 90 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **HTTP error sending the FCM message to the FCM server** | 4139 | KLSRV_GCM_HTTP_ERROR | Events of this type occur when Mobile Device Management is configured to use Google Firebase Cloud Messaging (FCM) for connecting managed mobile devices with the Android operating system and FCM Server reverts to the Administration Server a request with a HTTP code other than 200 (OK).<br>Following might be the causes and appropriate responses to the event:<br>• Problems on the FCM server side. Read the HTTP code in the details of the event and respond accordingly. For more information on the HTTP codes received from FCM Server and related errors, please refer to the Google Firebase service documentation (see chapter "Downstream message error response codes").<br>• Problems on the proxy server side (if you use proxy server). Read the HTTP code in the details of the event and respond accordingly. | 90 days |
| **License limit has been exceeded** | 4098 | KLSRV_EV_LICENSE_CHECK_100_110 | Once a day Kaspersky Security Center Linux checks whether a licensing limit is exceeded.<br>Events of this type occur when Administration Server detects that some license limits are exceeded by Kaspersky applications installed on client devices and if the number of currently used licensing units covered by a single license constitute 100% to 110% of the total number of units covered by the license.<br>Even when this event occurs, client devices are protected.<br>You can respond to the event in the following ways:<br>• Look through the managed devices list. Delete devices that are not in use.<br>• Provide a license for more devices (add a valid activation code or a key file to Administration Server).<br>Kaspersky Security Center Linux determines the rules to generate events when a licensing limit is exceeded. | 90 days |
| **Limit of installations will soon be reached for one of the licensed applications groups** | 4128 | KLSRV_INVLICPROD_EXPIRED_SOON | Events of this type occur when one of the license keys for third-party applications included in a licensed applications group is about to expire. As a result, the installation limit for one of the groups will be reduced.<br>You can respond to the event in the following ways:<br>• If the third-party application is not in use on some of the managed devices, delete the application from these devices.<br>• If you expect that the number of installations for the third-party application will exceed the allowed maximum in the near future, consider obtaining a third-party license for a greater number of devices in advance.<br>You can manage license keys of third-party applications using the functionality of licensed applications groups. | 90 days |
| **New updates for Kaspersky application modules have been registered** | 4141 | KLSRV_SEAMLESS_UPDATE_REGISTERED | Events of this type occur when Administration Server registers new updates for the Kaspersky software installed on managed devices that require approval to be installed.<br>Approve or decline the updates by using Kaspersky Security Center Web Console. | 90 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **No free space in the Administration Server database** | 4106 | KLSRV_NO_SPACE_IN_DATABASE | Events of this type occur if space in the Administration Server database is too limited. If you do not remedy the situation, soon the Administration Server database will reach its capacity and Administration Server will not function.<br>Following are the causes of this event, depending on the DBMS that you use, and the appropriate responses to the event.<br>• Do not limit the number of events to store in the Administration Server database<br>• Reduce the list of events to store in the Administration Server database<br>Review the information on DBMS selection. | 90 days |
| **The limit on the number of events in the database is exceeded, deletion of events has started** | 4145 | KLSRV_EVP_DB_TRUNCATING | Events of this type occur when deletion of old events from the Administration Server database has started after the Administration Server database capacity is reached.<br>You can respond to the event in the following ways:<br>• Change the maximum number of events stored in the Administration Server database<br>• Reduce the list of events to store in the Administration Server database | Not stored |
| **The limit on the number of events in the database is exceeded, the events have been deleted** | 4146 | KLSRV_EVP_DB_TRUNCATED | Events of this type occur when old events have been deleted from the Administration Server database after the Administration Server database capacity is reached.<br>You can respond to the event in the following ways:<br>• Change the allowed maximum number of events to be stored in the Administration Server database<br>• Reduce the list of events to store in the Administration Server database | Not stored |

## Administration Server informational events

The table below shows the events of Administration Server that have the **Info** importance level.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. For Administration Server, you can additionally view and configure the event list in the Administration Server properties. If you want to configure notification settings for all the events at once, configure general notification settings in the Administration Server properties.

Administration Server informational events

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Administration Server certificate for mobile devices is being renewed** | 6127 | KLSRV_EV_SRV_CERT_RENEWED | This event occurs when the Administration Server certificate has been renewed. | 30 days |
| **Audit: Command has been sent to device** | 4170 | KLAUD_EV_COMMAND_SENT | Events of this type occur when the user sends a command to the mobile device. | 30 days |
| **Audit: Connection to Administration Server has been terminated** | 4151 | KLAUD_EV_SERVERDISCONNECT | | 30 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Audit: Connection to the Administration Server has been established** | 4147 | KLAUD_EV_SERVERCONNECT | Events of this type occur when a user connects to Administration Server by using Kaspersky Security Center Web Console. These events include the IP address of the device where the Kaspersky Security Center Web Console Server is installed. | 30 days |
| **Audit: Custom parameter has been created** | 4167 | KLAUD_EV_CUSTOM_PARAMETER_CREATED | Events of this type occur when a user creates a new custom parameter. | 30 days |
| **Audit: Custom parameter has been deleted** | 4168 | KLAUD_EV_CUSTOM_PARAMETER_DELETED | Events of this type occur when a user deletes a custom parameter. | 30 days |
| **Audit: Custom parameter settings have been modified** | 4169 | KLAUD_EV_CUSTOM_PARAMETER_CHANGED | Events of this type occur when a user modifies settings of a custom parameter. | 30 days |
| **Audit: Custom parameter values have been changed** | 4166 | KLAUD_EV_CUSTOM_PARAMETERS_VALUE_CHANGED_BY_ADMIN | Events of this type occur when a user sets or changes the values of one or more custom parameters on an Android device using Kaspersky Security Center Web Console. | 30 days |
| **Audit: Encryption keys imported/exported** | 5100 | KLAUD_EV_DPEKEYSEXPORT | For example, this event occurs during migration. | 30 days |
| **Audit: Group settings have been modified** | 4149 | KLAUD_EV_ADMGROUP_CHANGED | Events of this type occur when a security group has been edited. | 30 days |
| **Audit: Object has been modified** | 4148 | KLAUD_EV_OBJECTMODIFY | This event tracks changes in the following objects:<br>• Administration group<br>• Security group<br>• User<br>• Managed device<br>• Package<br>• Task<br>• Policy<br>• Server<br>• Virtual Server | 30 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Audit: Object properties have been modified** | 4152 | KLAUD_EV_OBJECTPROPMODIFIED | This event tracks changes in the following properties:<br>• User<br>• License<br>• Server<br>• Virtual server | 30 days |
| **Audit: Object status has changed** | 4150 | KLAUD_EV_TASK_STATE_CHANGED | For example, this event occurs when a task has failed with an error. | 30 days |
| **Audit: Test connection to SIEM server succeeded** | 5110 | KLAUD_EV_SIEM_TEST_SUCCESS | Events of this type occur when a test connection to the SIEM server succeeded. | 30 days |
| **Audit: User permissions have been modified** | 4153 | KLAUD_EV_OBJECTACLMODIFIED | This event occurs when user permissions have been modified | 30 days |
| **Connection to the primary Administration Server has been established** | 4117 | KLSRV_EV_MASTER_SRV_CONNECTED | | 30 days |
| **Connection to the secondary Administration Server has been established** | 4115 | KLSRV_EV_SLAVE_SRV_CONNECTED | Refer to the following article for details: Creating a hierarchy of Administration Servers: adding a secondary Administration Server. | 30 days |
| **Databases have been updated** | 4144 | KLSRV_UPD_BASES_UPDATED | Events of this type occur when the **Download updates to the Administration Server repository** task finishes updating databases. | 30 days |
| **Device has been automatically moved according to a rule** | 1074 | KLSRV_HOST_MOVED_WITH_RULE_EX | Events of this type occur when devices have been moved to administration groups by using device moving rules. A separate event is published for each moved device. | 30 days |
| **Device has been removed from the group: inactive on the network for a long time** | 4104 | KLSRV_INVISIBLE_HOSTS_REMOVED | Events of this type occur when devices have been automatically removed from a group for inactivity. | 30 days |
| **FCM Instance ID has changed on this mobile device** | 4137 | KLSRV_GCM_DEVICE_REGID_CHANGED | Events of this type occur when the Firebase Cloud Messaging token has changed on the device.<br>For information on the FCM token rotation, please refer to the Firebase service documentation. | 30 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **File uploaded to Administration Server** | 4162 | KLSRV_FILE_UPLOADED | Events of this type occur if the administrator has uploaded a file to the list in Web Console: **Asset management → Mobile → Apps & files → Files**. | 30 days |
| **File deleted from Administration Server** | 4163 | KLSRV_FILE_REMOVED | Events of this type occur if the administrator has deleted a file from the list in Web Console: **Asset management → Mobile → Apps & files → Files**. | 30 days |
| **File downloaded to device** | 4164 | KLSRV_FILE_DOWNLOADED | This event occurs in the following cases:<br>• The administrator has downloaded a file to the administrator's workstation from the list in the Web Console: **Asset management → Mobile → Apps & files → Files**.<br>• A file from the **Asset management → Mobile → Apps & files → Files** list has been downloaded to a device on which Kaspersky Endpoint Security for Android is installed. | 30 days |
| **Failed to download file to device** | 4165 | KLSRV_FILE_DOWNLOAD_FAILED | Events of this type occur in the following cases:<br>• An error occurred when the administrator tried to download a file to the administrator's workstation from the list in Web Console: **Asset management → Mobile → Apps & files → Files**.<br>• An error occurred while downloading a file from the **Asset management → Mobile → Apps & files → Files** list to a device on which Kaspersky Endpoint Security for Android is installed. | 30 days |
| **Files have been found to send to Kaspersky for analysis** | 4131 | KLSRV_APS_FILE_APPEARED | | 30 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Limit of installations will soon be exceeded (more than 90% is used up) for one of the licensed applications groups** | 4127 | KLSRV_INVLICPROD_FILLED | Events of this type occur when the number of installations for third-party applications included in a licensed applications group reaches 90% of the maximum allowed value specified in the license key properties.<br>You can respond to the event in the following ways:<br>• If the third-party application is not in use on some of the managed devices, delete the application from these devices.<br>• If you expect that the number of installations for the third-party application will exceed the allowed maximum in the near future, consider obtaining a third-party license for a greater number of devices in advance.<br>You can manage license keys of third-party applications using the functionality of licensed applications groups. | 30 days |
| **New device has been detected** | 4100 | KLSRV_EVENT_HOSTS_NEW_DETECTED | Events of this type occur when new networked devices have been discovered. | 30 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Over 90% of the license key is used up** | 4097 | KLSRV_EV_LICENSE_CHECK_90 | Events of this type occur when Administration Server detects that some license limits are exceeded by Kaspersky applications installed on client devices and if the number of currently used licensing units covered by a single license exceeds 90% of the total number of units covered by the license.<br>Even when a licensing limit is exceeded, client devices are protected.<br>You can respond to the event in the following ways:<br>• Look through the managed devices list. Delete devices that are not in use.<br>• Provide a license for more devices (add a valid activation code or a key file to Administration Server).<br>Kaspersky Security Center Linux determines the rules to generate events when a licensing limit is exceeded. | 30 days |
| **Reserve Administration Server certificate for mobile devices has been created** | 6126 | KLSRV_EV_SRV_CERT_RESERVE_CREATED | This event occurs when an Administration Server certificate has been created. | 30 days |
| **Updates have been successfully copied to the specified folder** | 4122 | KLSRV_UPD_REPL_OK | Events of this type occur when the **Download updates to the Administration Server repository** task finishes copying files to a specified folder. | 30 days |

The events **Reserve certificate created** and **Certificate renewing** are automatically published by Administration Server and displayed in Administration Console only when the operations corresponding to these events are performed for Administration Server certificates for mobile devices and UEFI devices.

# Network Agent events

This section contains information about the events related to Network Agent.

## Network Agent functional failure events

The table below shows the events of Kaspersky Security Center Linux Network Agent that have the **Functional failure** severity level.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. If you want to configure notification settings for all the events at once, configure general notification settings in the Administration Server properties.

Network Agent functional failure events

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Failed to install root certificates** | 7728 | KLNAG_EV_ROOT_CERT_INSTALL_ERR | The event contains the description of the certificates installation error. | 30 days |
| **Failed to install third-party software update** | 7697 | KLNAG_EV_3P_PATCH_INSTALL_ERROR | Events of this type occur if the Vulnerability and patch management feature is in use, and if update of third-party software was not successful.<br>Check whether the link to the third-party software is valid. Read the event description. | 30 days |
| **Failed to install Windows updates** | 7717 | KLNAG_EV_WUA_INSTALL_ERROR | Events of this type occur if Windows Updates were not successful.<br>Read the event description. Look for the error in the Microsoft Knowledge Base. Contact Microsoft Technical Support if you cannot resolve the issue yourself. | 30 days |
| **Failed to remove root certificates** | 7730 | KLNAG_EV_ROOT_CERT_REMOVE_ERR | The event contains the description of the certificates removal error. | 30 days |
| **Failed to restore sudoers file to reference value** | 7726 | KLNAG_EV_SUDOER_RESTORED_ERR | The event contains the description of the sudoers file replacement error. | 30 days |
| **Update installation error** | 7702 | KLNAG_EV_PATCH_INSTALL_ERROR | Events of this type occur if automatic updating and patching for Kaspersky Security Center Linux components was not successful. The event does not concern updates of the managed Kaspersky applications.<br>Read the event description. A Windows issue on the Administration Server might be a reason for this event. If the description mentions any issue of Windows configuration, resolve this issue. | 30 days |
| **User management: errors** | 7723 | KLNAG_EV_USR_MNG_ERR | General warning event. | 30 days |

## Network Agent warning events

The table below shows the events of Network Agent that have the **Warning** severity level.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. If you want to configure notification settings for all the events at once, configure general notification settings in the Administration Server properties.

Network Agent warning events

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **KSN Proxy has started. Failed to check KSN for availability** | 7718 | KSNPROXY_STARTED_CON_CHK_FAILED | Events of this type occur when test connection fails for the configured KSN proxy connection. | 30 days |
| **Security issue has occurred** | 549 | GNRL_EV_APP_INCIDENT_OCCURED | Events of this type occur when an incident has been found on a device. For example, this event occurs when the device has low disk space. | 30 days |
| **Sudoers file found does not match reference value** | 7724 | KLNAG_EV_SUDOER_DIFFERENT | Events of this type occur when there is a mismatch between the sudoers file and the reference file. | 30 days |

| Event type display name | Event type ID | Event type | Description | Default storage term |
|---|---|---|---|---|
| **Third-party software update installation has been postponed** | 7698 | KLNAG_EV_3P_PATCH_INSTALL_SLIPPED | For example, events of this type occur when EULA for a third-party update installation is declined. | 30 days |
| **Third-party software update installation has completed with a warning** | 7696 | KLNAG_EV_3P_PATCH_INSTALL_WARNING | Download the trace files and check the KLRI_PATCH_RES_DESC field value for details. | 30 days |
| **User management: warnings** | 7722 | KLNAG_EV_USR_MNG_WRN | General warning event. | 30 days |
| **Warning has been returned during installation of the software module update** | 7701 | KLNAG_EV_PATCH_INSTALL_WARNING | Download the trace files and check the KLRI_PATCH_RES_DESC field value for details. | 30 days |

## Network Agent informational events

The table below shows the events of Network Agent that have the **Info** severity level.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. If you want to configure notification settings for all the events at once, configure general notification settings in the Administration Server properties.

Network Agent informational events

| Event type display name | Event type ID | Event type | Default storage term |
|---|---|---|---|
| **Application has been installed** | 7703 | KLNAG_EV_INV_APP_INSTALLED | 30 days |
| **Application has been uninstalled** | 7704 | KLNAG_EV_INV_APP_UNINSTALLED | 30 days |
| **Certificate received for Web Server HTTPS port** | — | WEB_SERVER_CERTIFICATE_RENEWED | 30 days |
| **Device has been authorized** | 7711 | KLNAG_EV_NAC_HOST_AUTHORIZED | 30 days |
| **New device has been detected** | 7710 | KLNAG_EV_NAC_DEVICE_DISCOVERED | 30 days |
| **Device has been removed** | 7709 | KLNAG_EV_DEVICE_REMOVE | 30 days |
| **Installation of the software module update has started** | 7700 | KLNAG_EV_PATCH_INSTALL_STARTING | 30 days |
| **KSN Proxy has started. KSN availability check has completed successfully** | 7719 | KSNPROXY_STARTED_CON_CHK_OK | 30 days |
| **KSN Proxy has stopped** | 7720 | KSNPROXY_STOPPED | 30 days |
| **Monitored application has been installed** | 7705 | KLNAG_EV_INV_OBS_APP_INSTALLED | 30 days |
| **Monitored application has been uninstalled** | 7706 | KLNAG_EV_INV_OBS_APP_UNINSTALLED | 30 days |
| **New device has been added** | 7708 | KLNAG_EV_DEVICE_ARRIVAL | 30 days |
| **Root certificates installed** | 7727 | KLNAG_EV_ROOT_CERT_INSTALLED | 30 days |
| **Root certificates removed** | 7729 | KLNAG_EV_ROOT_CERT_REMOVED | 30 days |
| **Sudoers file successfully restored to reference value** | 7725 | KLNAG_EV_SUDOER_RESTORED | 30 days |
| **Third-party application has been installed** | 7707 | KLNAG_EV_INV_CMPTR_APP_INSTALLED | 30 days |
| **Third-party software update has been installed successfully** | 7694 | KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY | 30 days |
| **Third-party software update installation has started** | 7695 | KLNAG_EV_3P_PATCH_INSTALL_STARTING | 30 days |

| Event type display name | Event type ID | Event type | Default storage term |
|---|---|---|---|
| **Update for software modules has been installed successfully** | 7699 | KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY | 30 days |
| **User management: info** | 7721 | KLNAG_EV_USR_MNG_INF | 30 days |
| **Web Server started on host** | — | WEB_SERVER_STARTED | 30 days |
| **Web Server stopped on host** | — | WEB_SERVER_STOPPED | 30 days |
| **Windows Desktop Sharing: Application has been started** | 7714 | KLUSRLOG_EV_PROCESS_LAUNCHED | 30 days |
| **Windows Desktop Sharing: File has been modified** | 7713 | KLUSRLOG_EV_FILE_MODIFIED | 30 days |
| **Windows Desktop Sharing: File has been read** | 7712 | KLUSRLOG_EV_FILE_READ | 30 days |
| **Windows Desktop Sharing: Started** | 7715 | KLUSRLOG_EV_WDS_BEGIN | 30 days |
| **Windows Desktop Sharing: Stopped** | 7716 | KLUSRLOG_EV_WDS_END | 30 days |

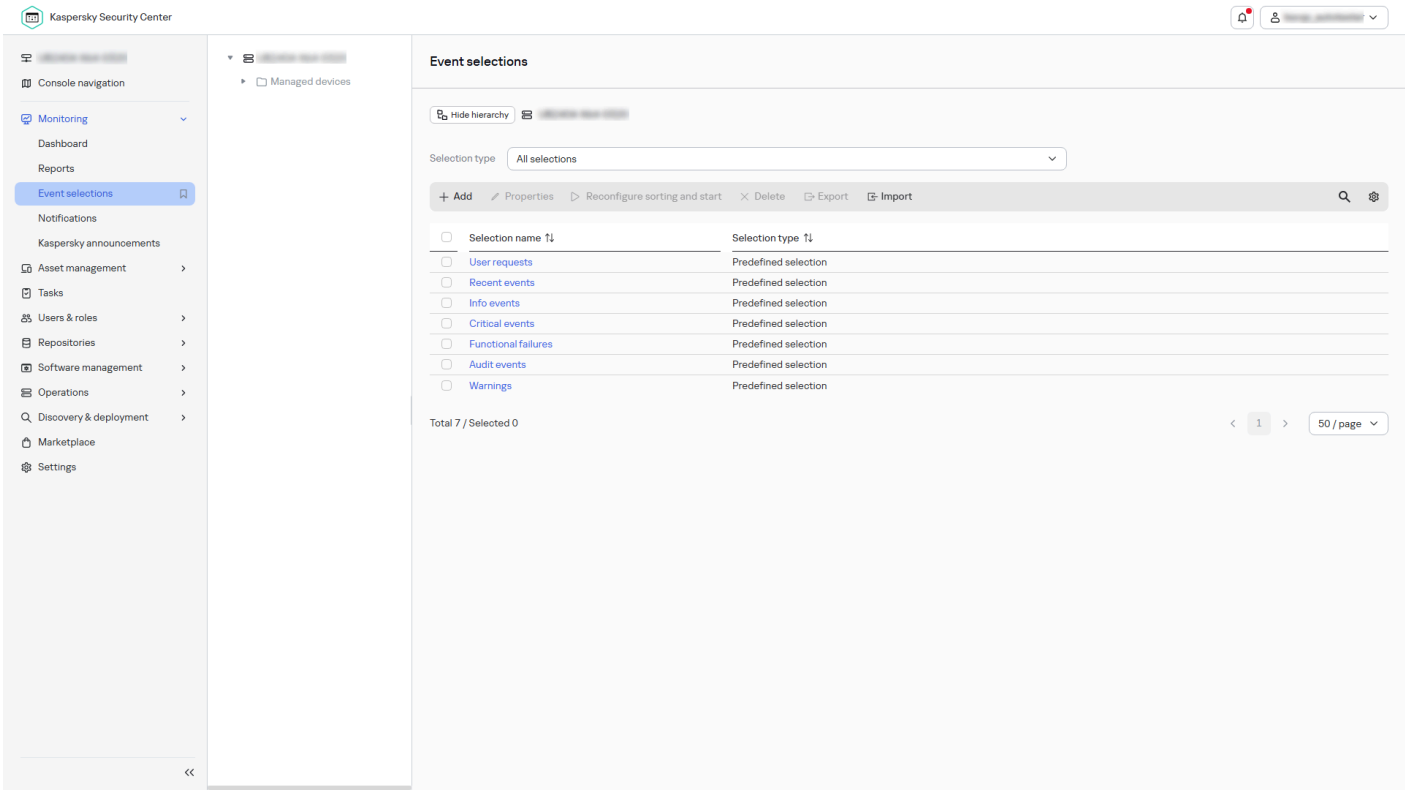
# Using event selections

Event selections provide an onscreen view of named sets of events that are selected from the Administration Server database. These sets of events are grouped according to the following categories:

- By importance level—**Critical events**, **Functional failures**, **Warnings**, and **Info events**
- By time—**Recent events**
- By type—**User requests** and **Audit events**

You can create and view user-defined event selections based on the settings available, in the Kaspersky Security Center Web Console interface, for configuration.

Event selections are available in the Kaspersky Security Center Web Console, in the **Monitoring** section, by clicking **Event selections**.




The list of event selections

By default, event selections include information for the last seven days.

Kaspersky Security Center Linux has a default set of event (predefined) selections:

- Events with different importance levels:
  - **Critical events**
  - **Functional failure**
  - **Warnings**
  - **Info events**
- **User requests** (events of managed applications)
- **Recent events** (over the last week)
- Audit events.

You can also create and configure additional user-defined selections. In user-defined selections, you can filter events by the properties of the devices they originated from (device names, IP ranges, and administration groups), by event types and severity levels, by application and component name, and by time interval. It is also possible to include task results in the search scope. You can also use a simple search field where a word or several words can be typed. All events that contain any of the typed words anywhere in their attributes (such as event name, description, component name) are displayed.

Both for predefined and user-defined selections, you can limit the number of displayed events or the number of records to search. Both options affect the time it takes Kaspersky Security Center Linux to display the events. The larger the database is, the more time-consuming the process can be.

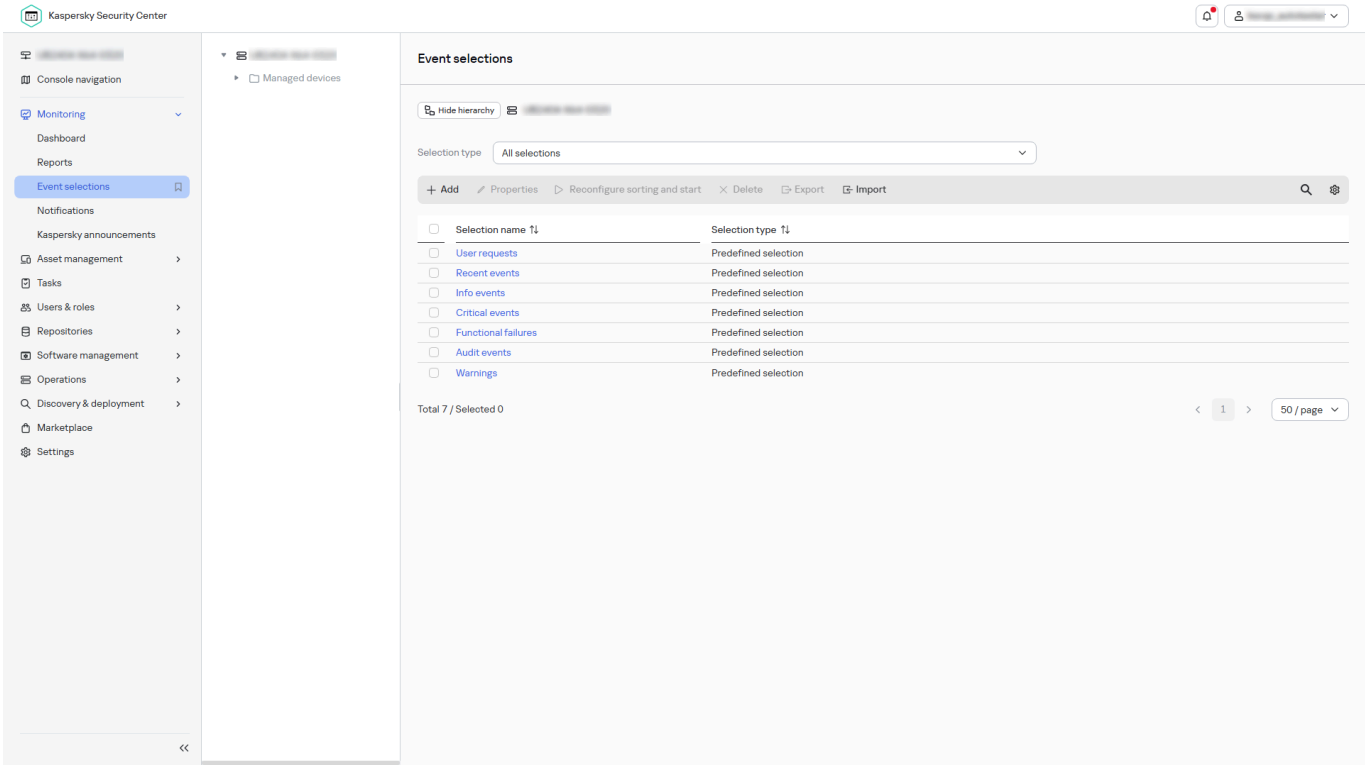
You can do the following:

- Edit properties of event selections
- Generate event selections
- View details of event selections
- Delete event selections
- Delete events from the Administration Server database

# Creating an event selection

*To create an event selection:*

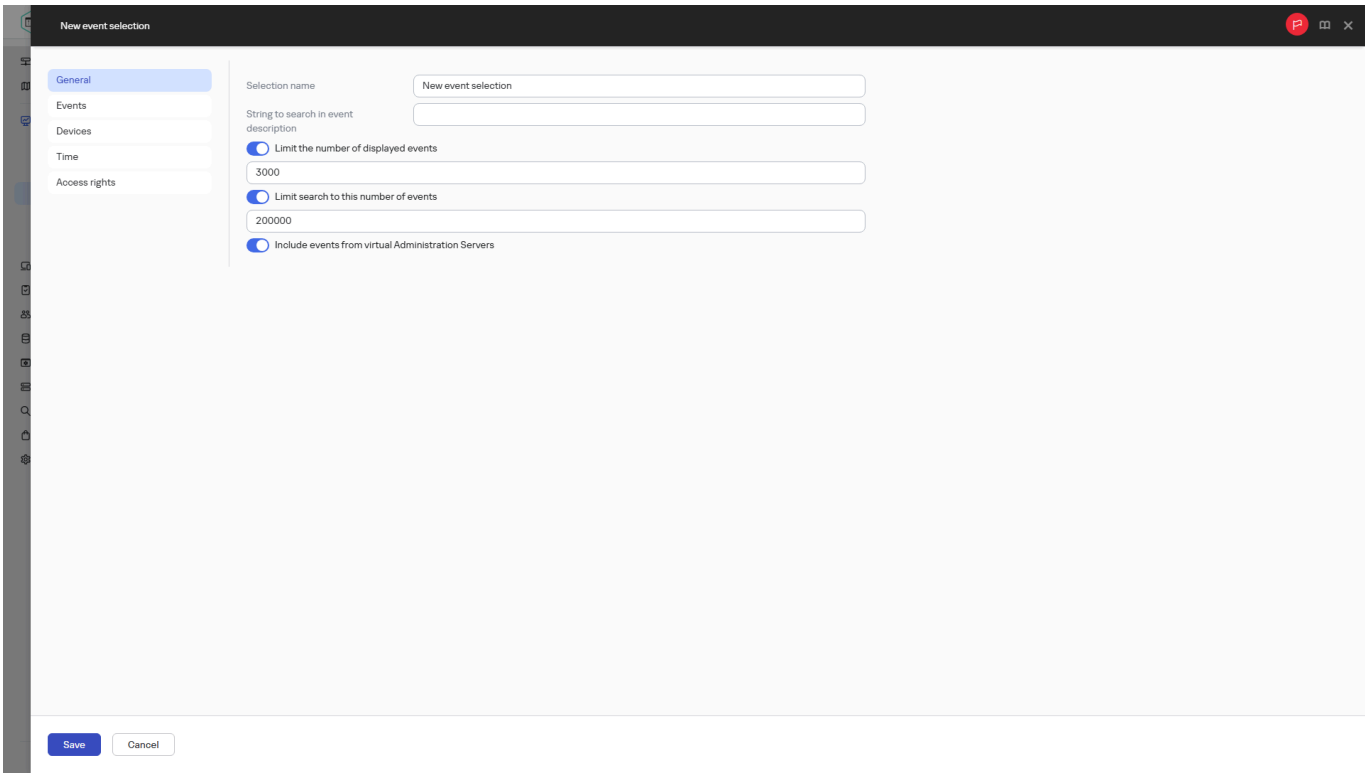
1. In the main menu, go to the **Monitoring** → **Event selections**.




The list of event selections

2. Click **Add**.

3. In the **New event selection** window that opens, specify the settings of the new event selection. Do this in one or more of the sections in the window.




Creating a new event selection

4. Click **Save** to save changes.

   A confirmation window opens.

5. To view the event selection result, keep the **Go to selection result** check box selected.

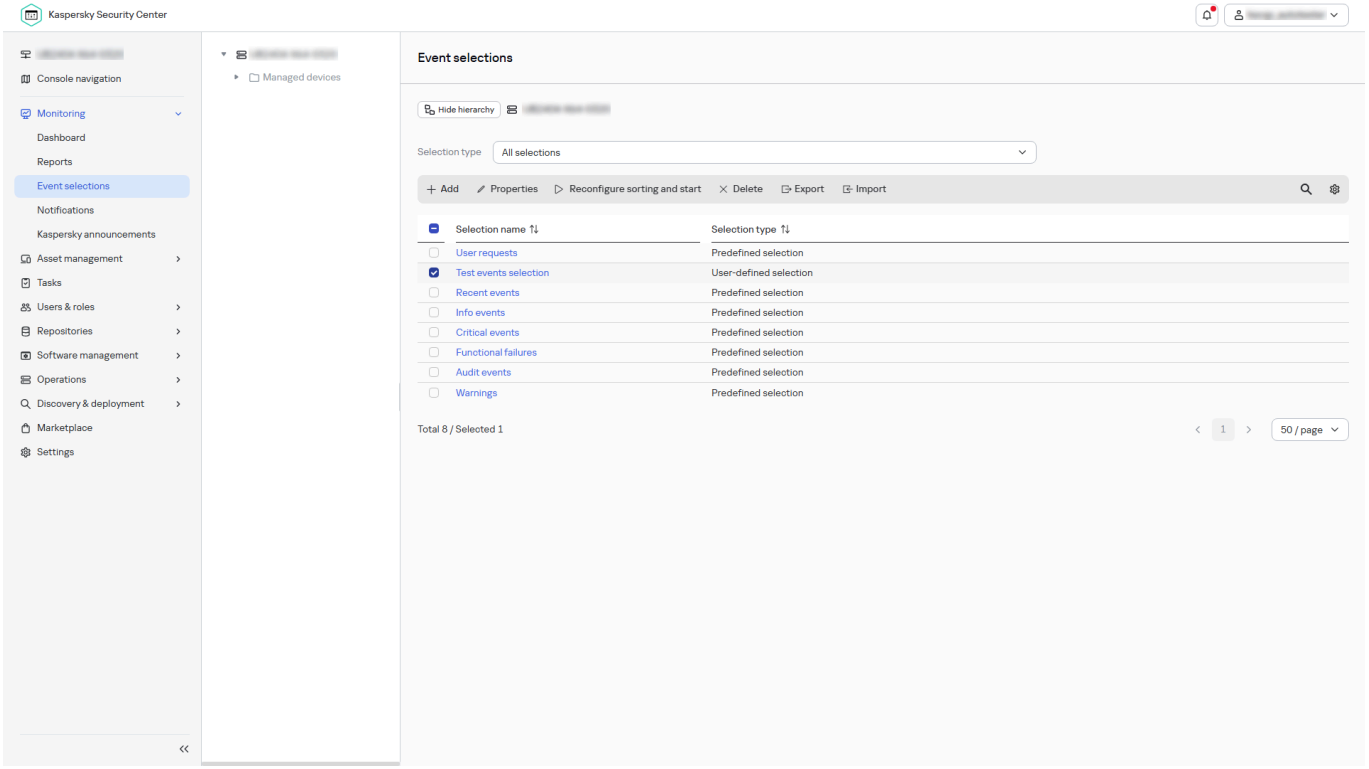
6. Click **Save** to confirm the event selection creation.

If you kept the **Go to selection result** check box selected, the event selection result is displayed. Otherwise, the new event selection appears in the list of event selections.

# Editing an event selection

*To edit an event selection:*

1. In the main menu, go to **Monitoring** → **Event selections**.
2. Select the check box next to the event selection that you want to edit.




The list of event selections

3. Click the **Properties** button.

   An event selection settings window opens.

4. Edit the properties of the event selection.

   For predefined event selections, you can edit only the properties on the following tabs: **General** (except for the selection name), **Time**, and **Access rights**.

   For user-defined selections, you can edit all properties.

5. Click **Save** to save changes.

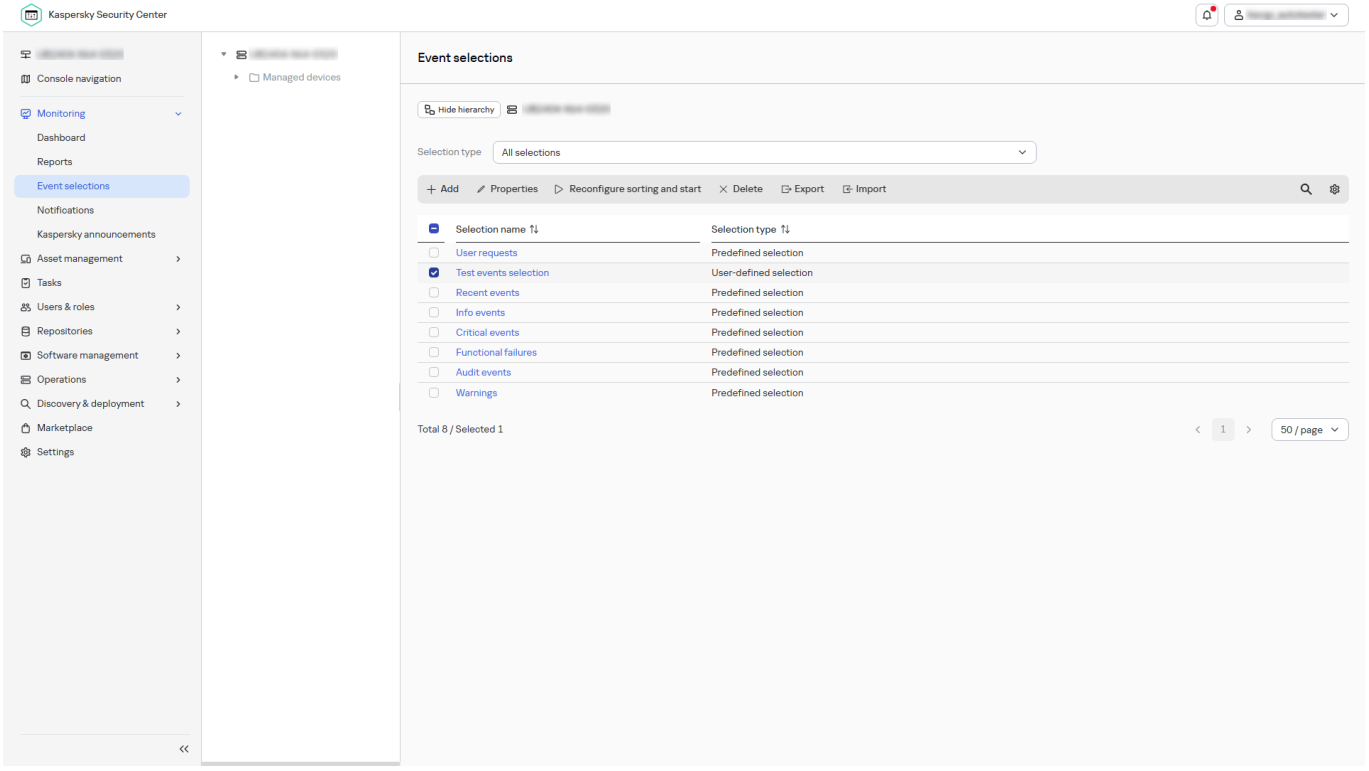
The edited event selection is shown in the list.

# Viewing a list of an event selection

*To view an event selection:*

1. In the main menu, go to the **Monitoring** → **Event selections**.

2. Select the check box next to the event selection that you want to start.



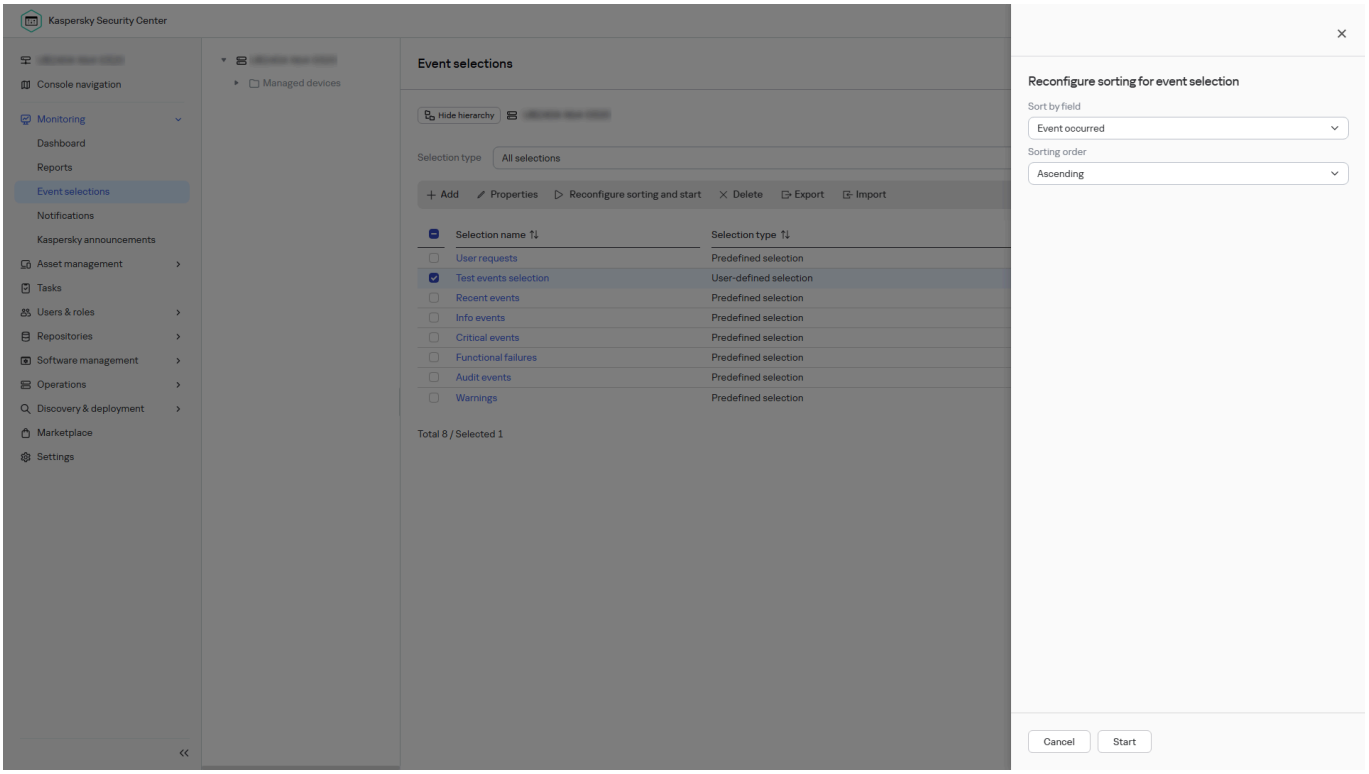

The list of event selections

3. Do one of the following:

- If you want to configure sorting in the event selection result, do the following:

  a. Click the **Reconfigure sorting and start** button.

  b. In the displayed **Reconfigure sorting for event selection** window, specify the sorting settings.

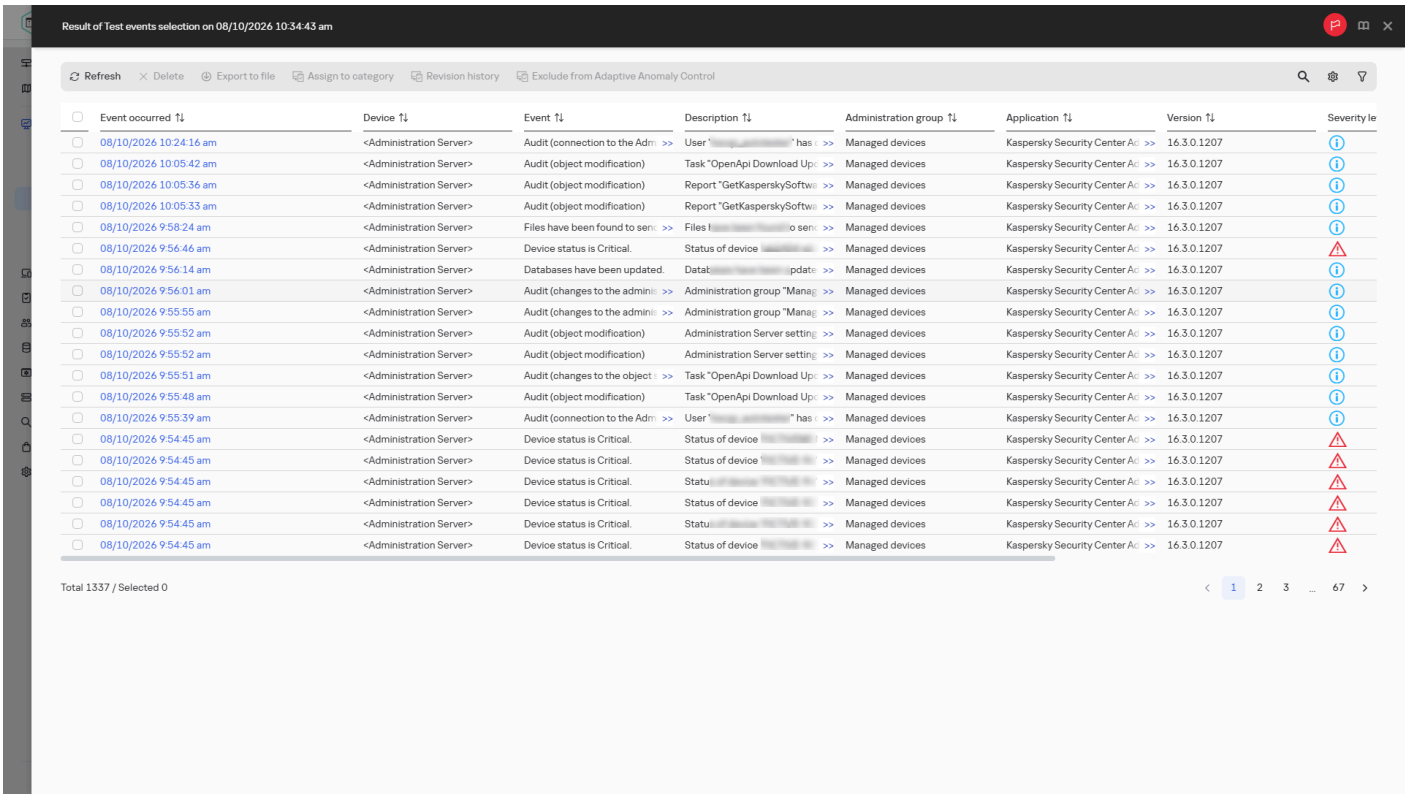



Specifying the sorting settings of the event selection

  a. Click the name of the selection.

- Otherwise, if you want to view the list of events as they are sorted on the Administration Server, click the name of the selection.

The event selection result is displayed.




The event selection result

# Exporting an event selection

Kaspersky Security Center Linux allows you to save an event selection and its settings to a KLO file. You can use this KLO file to import the saved event selection both to Kaspersky Security Center Windows and Kaspersky Security Center Linux.

Note that you can export only user-defined event selections. Event selections from the default set of Kaspersky Security Center Linux (predefined selections) cannot be saved to a file.

*To export an event selection:*

1. In the main menu, go to **Monitoring** → **Event selections**.
2. Select the check box next to the event selection that you want to export.

   You cannot export multiple event selections at the same time. If you select more than one selection, the **Export** button will be disabled.
3. Click the **Export** button.
4. In the opened **Save as** window, specify the event selection file name and path, and then click the **Save** button.

   The **Save as** window is displayed only if you use Google Chrome, Microsoft Edge, or Opera. If you use another browser, the event selection file is automatically saved in the **Downloads** folder.

# Importing an event selection

Kaspersky Security Center Linux allows you to import an event selection from a KLO file. The KLO file contains the exported event selection and its settings.

*To import an event selection:*

1. In the main menu, go to **Monitoring** → **Event selections**.
2. Click the **Import** button, and then choose an event selection file that you want to import.
3. In the opened window, specify the path to the KLO file, and then click the **Open** button. Note that you can select only one event selection file.

   The event selection processing starts.

The notification with the import results appears. If the event selection is imported successfully, you can click the **View import details** link to view the event selection properties.

After a successful import, the event selection is displayed in the selection list. The settings of the event selection are also imported.

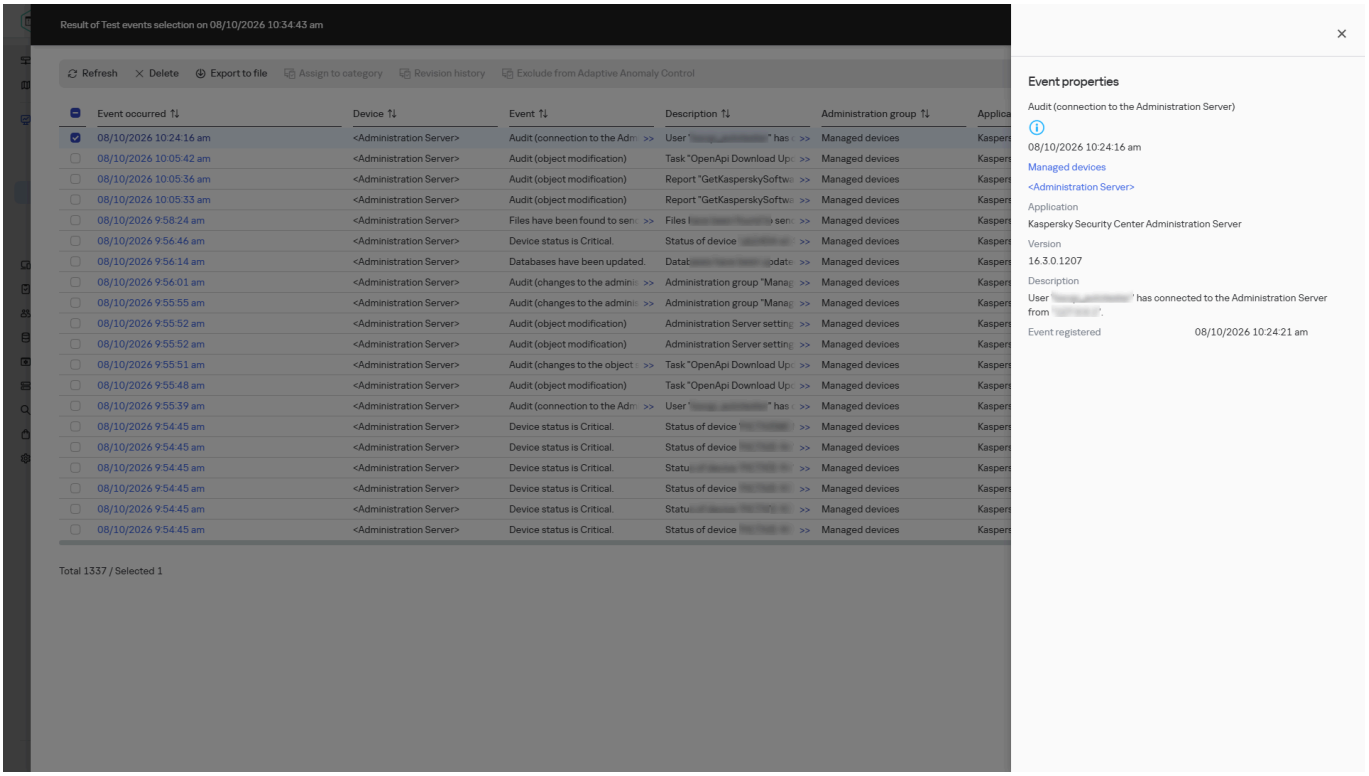
If the newly imported event selection has a name identical to that of an existing event selection, the name of the imported selection is expanded with the **(<next sequence number>)** index, for example: **(1)**, **(2)**.

# Viewing details of an event

*To view details of an event:*

1. Start an event selection.
2. Click the time of the required event.

The **Event properties** window opens.




The event properties window

3. In the displayed window, you can do the following:

   - View the information about the selected event
   - Go to the device on which the event occurred
   - Go to the administration group that includes the device on which the event occurred
   - For an event related to a task, go to the task properties

# Exporting events to a file

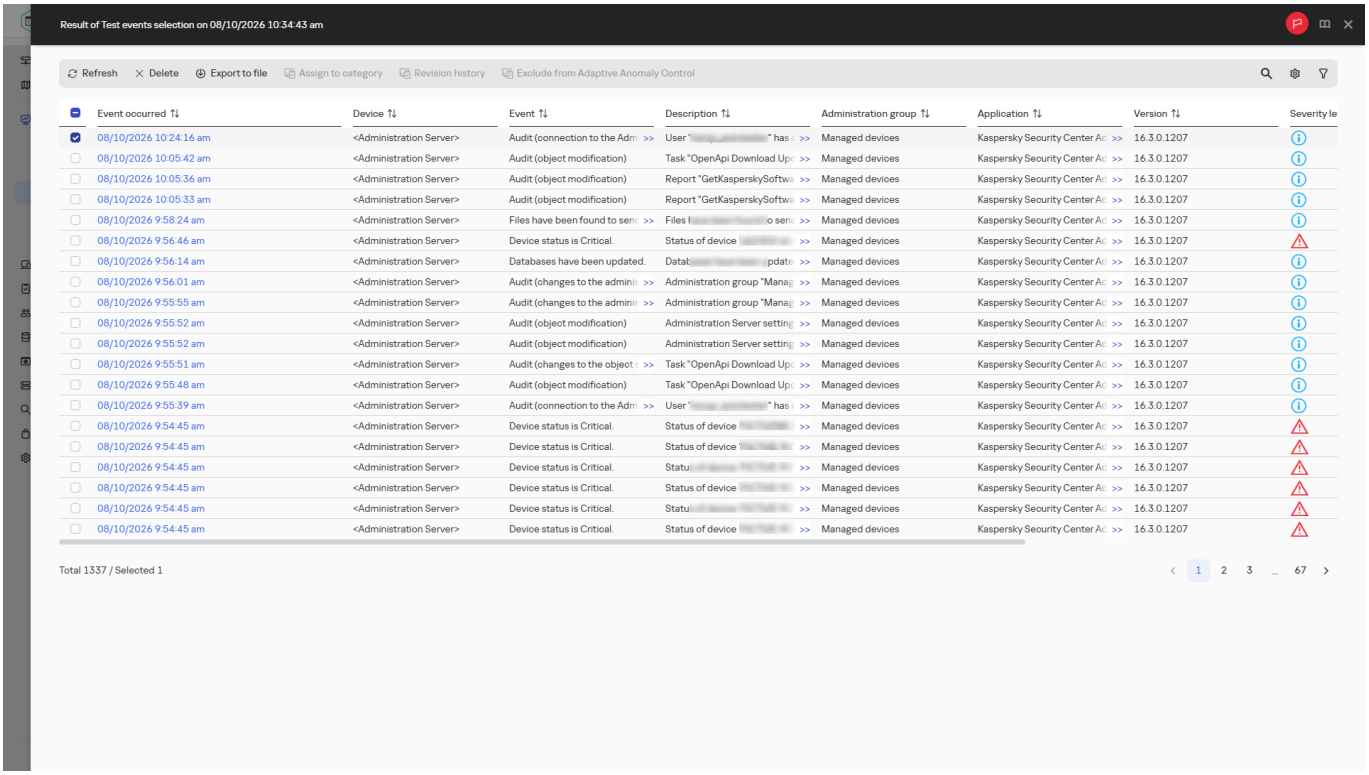
Kaspersky Security Center Linux can save events to a CSV or TXT file.

*To export events from an event selection:*

1. In the main menu, go to the **Monitoring** → **Event selections**.
2. Click the name of the selection that you need.

3. Select the events:

- If you want to export one or several events, select the check boxes next to the events.
- If you want to export all events on current page, select the check box above the list of events and click **Select all on current page**.
- If you want to export all events from a selection, select the check box above the list of events and click **Select all**.




The event selection result

4. Click the **Export** button and select **Export to CSV** or **Export to TXT**.

*To export events from the list of events on a device:*

1. Open the device list.
   - For managed devices: **Asset management** → **Managed devices**.
   - For unassigned devices: **Asset management** → **Unassigned devices**.
2. In the list of devices, click the link with the name of the required device, and then go to the **Events** tab.

3. Select the events:

   - If you want to delete one or several events, select the check boxes next to it.
   - If you want to delete all events on current page, select the check box above the list of events and click the **Select all on current page** option.
   - If you want to delete all events from a selection, select the check box above the list of events and click the **Select all** option.

4. Click the **Export** button and select **Export to CSV** or **Export to TXT**.

All information about the selected events included in the table is exported.

# Viewing an object history from an event

From an event of creation or modification of an object that supports revision management, you can switch to the revision history of the object.

*To view an object history from an event:*

1. Start an event selection.
2. Select the check box next to the required event.
3. Click the **Revision history** button.

The revision history of the object is opened.

# Deleting events

*To delete events from an event selection:*

1. Start an event selection.
2. Select the events:

   - If you want to delete one or several events, select the check boxes next to it.
   - If you want to delete all events on current page, select the check box above the list of events and click the **Select all on current page** option.
   - If you want to delete all events from a selection, select the check box above the list of events and click the **Select all** option.

3. Then click the **Delete** button.
4. In the window that opens, click **Delete**.

*To delete events from a device events list:*

1. Open the device list.
   - For managed devices: **Asset management** → **Managed devices**.
   - For unassigned devices: **Asset management** → **Unassigned devices**.
2. In the list of devices, click the link with the name of the required device, and then go to the **Events** tab.
3. Select the events:
   - If you want to delete one or several events, select the check boxes next to it.
   - If you want to delete all events on current page, select the check box above the list of events and click the **Select all on current page** option.
   - If you want to delete all events from a selection, select the check box above the list of events and click the **Select all** option.
4. Click **Delete**, and then confirm the action.
5. In the window that opens, click **Delete**.

   The selected events are deleted and cannot be restored.

# Deleting event selections

You can delete only user-defined event selections. Predefined event selections cannot be deleted.

*To delete one or several event selections:*

1. In the main menu, go to **Monitoring** → **Event selections**.
2. Select the check boxes next to the event selections that you want to delete.
3. Then click the **Delete** button.
4. In the window that opens, click **OK**.

   The event selection is deleted.

# Setting the storage term for an event

Kaspersky Security Center Linux allows you to receive information about events that occur during the operation of Administration Server and Kaspersky applications installed on managed devices. Information about events is saved in the Administration Server database. You might need to store some events for a longer or shorter period than specified by default values. You can change the default settings of the storage term for an event.

If you are not interested in storing some events in the database of Administration Server, you can disable the appropriate setting in the Administration Server policy and Kaspersky application policy, or in the Administration Server properties (only for Administration Server events). This will reduce the number of event types in the database.

The longer the storage term for an event, the faster the database reaches its maximum capacity. However, a longer storage term for an event lets you perform monitoring and reporting tasks for a longer period.

*To set the storage term for an event in the database of Administration Server:*

1. In the main menu, go to **Asset management** → **Policies**.
2. Click the name of the required policy.

   You can select a policy of a managed Kaspersky application, Network Agent, or Administration Server. For Administration Server, you can also configure the storage term of the events by clicking the Administration Server name.
3. Select the **Event configuration** tab.

   A list of event types related to the **Critical** section is displayed. If necessary, you can move to the **Functional failure**, **Warning**, or **Info** section.
4. In the list of event types in the right pane, click the link for the event whose storage term you want to change.

   In the **Event registration** section of the window that opens, the **Store in the Administration Server database for (days)** toggle button is enabled.
5. In the edit box below this toggle button, enter the number of days to store the event.
6. If you do not want to store an event in the Administration Server database, disable the **Store in the Administration Server database for (days)** option.

   > If you configure Administration Server events in Administration Server properties window and if event settings are locked in the Administration Server policy, you cannot redefine the storage term value for an event.
7. Click **OK**, and then after the right pane is closed, click the **Save** button.

   The properties window of the policy is closed.

From now on, when Administration Server receives and stores the events of the selected type, they will have the changed storage term. Administration Server does not change the storage term of previously received events.

# Blocking frequent events

This section provides information about managing frequent events blocking and about removing blocking of frequent events.

# About blocking frequent events

A managed application, for example, Kaspersky Endpoint Security for Linux, installed on a single or several managed devices can send a lot of events of the same type to the Administration Server. Receiving frequent events may overload the Administration Server database and overwrite other events. Administration Server starts blocking the most frequent events when the number of all the received events exceeds the specified limit for the database.

Administration Server blocks the frequent events from receiving automatically. You cannot block the frequent events yourself, or choose which events to block.

If you want to find out if an event is blocked, you can view the notification list or you can check if this event is present in the **Blocking frequent events** section of the Administration Server properties. If the event is blocked, you can do the following:

- If you want to prevent overwriting the database, you can continue blocking such type of events from receiving.
- If you want, for example, to find the reason of sending the frequent events to the Administration Server, you can unblock frequent events and continue receiving the events of this type anyway.
- If you want to continue receiving the frequent events until they become blocked again, you can remove from blocking the frequent events.

# Managing frequent events blocking

Administration Server blocks the automatic receiving of frequent events, but you can unblock and continue to receive frequent events. You can also block receiving frequent events that you unblocked before.

*To manage frequent events blocking:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Blocking frequent events** section.

3. In the **Blocking frequent events** section:

   - If you want to unblock the receiving of frequent events:

     a. Select the frequent events you want to unblock, and then click the **Exclude** button.

     b. Click **Save**.

   - If you want to block receiving frequent events:

     a. Select the frequent events you want to block, and then click the **Block** button.

     b. Click **Save**.

Administration Server receives the unblocked frequent events and does not receive the blocked frequent events.

## Removing blocking of frequent events

You can remove blocking for frequent events and start receiving them until Administration Server blocks these frequent events again.

*To remove blocking for frequent events:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Blocking frequent events** section.

3. In the **Blocking frequent events** section, select the frequent event types for which you want to remove blocking.

4. Click the **Remove from blocking** button.

The frequent event is removed from the list of frequent events. Administration Server will receive events of this type.

# Event processing and storage on the Administration Server

Information about events that occur during the operation of the application and managed devices is saved in the Administration Server database. Each event is attributed to a certain type and level of severity (*Critical event*, *Functional failure*, *Warning*, or *Info*). Depending on the conditions under which an event occurred, the application can assign different levels of severity to events of the same type.

You can view types and levels of severity assigned to events in the **Event configuration** section of the Administration Server properties window. In the **Event configuration** section, you can also configure processing of every event by the Administration Server:

- Registration of events on the Administration Server and in event logs of the operating system on a device and on the Administration Server.

- Method used for notifying the administrator of an event (for example, an SMS or email message).

In the **Events repository** section of the Administration Server properties window, you can edit the settings of events storage in the Administration Server database by limiting the number of event records and record storage term. When you specify the maximum number of events, the application calculates an approximate amount of storage space required for the specified number. You can use this approximate calculation to evaluate whether you have enough free space on the disk to avoid database overflow. The default capacity of the Administration Server database is 400,000 events. The maximum recommended capacity of the database is 45 million events.

The application checks the database every 10 minutes. If the number of events reaches the specified maximum value plus 10,000, the application deletes the oldest events so that only the specified maximum number of events remains.

When the Administration Server deletes old events, it cannot save new events to the database. During this period, information about events that were rejected is written to the operating system log. The new events are queued and then saved to the database after the deletion operation is complete. By default, the event queue is limited to 20,000 events. You can customize the queue limit by editing the KLEVP_MAX_POSTPONED_CNT flag value.

# Notifications and device statuses

This section contains information on how to view notifications, configure notification delivery, use device statuses, and enable changing device statuses.

## About notifications

Notifications inform you about important events and help you respond to them quickly by performing the recommended actions or any other appropriate actions.

Depending on the notification method chosen, the following types of notifications are available:

- Onscreen notifications
- Notifications by SMS
- Notifications by email
- Notifications by executable file or script

### Onscreen notifications

On-screen notifications are available in the drop-down panel that opens when you click the notifications icon ( ) and in Notification center. These get one of the following severity levels: **Critical**, **Warning**, **Info**, or **Success**.

If the notifications icon has a red dot, there are unread notifications.

On-screen notifications are grouped into the following types:

- **Attention required**

  Notifications that require your attention. Notifications in the **Critical** category are displayed on the main dashboard, in addition to Notification center.

- **System**

  System notifications. They are divided into the following categories:

  - **Deployment**
  - **Devices**
  - **Protection**
  - **Updates** (includes notifications about Kaspersky applications available for download, notifications about downloaded anti-virus database updates, and notifications about devices, if any, that require a restart after a Network Agent update)

- **Exploit Prevention**
- **Administration Server** (includes only events related to Administration Server)

- **Announcements**

  Notifications that provide information related to your version of Kaspersky Security Center Linux and the managed applications installed on managed devices.

You can monitor your organization's network by viewing on-screen notifications and responding to them in real time.

Notifications by email, by SMS, and by executable file or a script

Kaspersky Security Center Linux provides the capability to monitor your organization's network by sending notifications about any event that you consider important. For any event, you can configure notifications by email, by SMS, or by running an executable file or a script.

Upon receiving notifications by email or by SMS, you can decide on your response to an event. This response should be the most appropriate for your organization's network. By running an executable file or a script, you predefine a response to an event. You can also consider running an executable file or a script as a primary response to an event. After the executable file runs, you can take other steps to respond to the event.

# Viewing attention-required notifications

Attention-required notifications notify you about events that may require your attention. These get one of the following severity levels: **Critical**, **Warning**, **Info**, or **Success**.

Notifications in the **Critical** category are displayed in Web Console in addition to Notification center. If multiple critical notifications are available, Web Console displays a single notification showing the total number of critical notifications.

You can view attention required notifications in one of the following ways:

- In the drop-down panel

  Only unread attention-required notifications are displayed in the drop-down panel. If there are no unread attention required notifications, the **Attention required** tab is not displayed.

- In Notification center

  Notification center displays all attention-required notifications, including both read and unread notifications. If there are no attention required notifications, the **Attention required** tab is not displayed.

*To view attention-required notifications in the drop-down panel:*

1. At the top of Web Console, click the notification icon ( ).

   The **Notifications** drop-down panel opens.

2. On the **Attention required** tab, view unread notifications.

3. If necessary, mark attention-required notifications as read in one of the following ways:

   - To mark a notification as read, click the close icon ( × ) next to the notification.
   - To mark all notifications as read, click **Mark all as read**.

   After you review and mark attention-required notifications as read, the **Attention required** tab is no longer displayed in the **Notifications** drop-down panel. You can view all read attention-required notifications in Notification center.

*To view attention-required notifications in Notification center:*

1. At the top of Web Console, click the notification icon (  ).
2. In the **Notifications** drop-down panel that opens, click the **Go to Notification center** button.

   The **Notification center** window opens.
3. On the **Attention required** tab, select one of the following sections:

   - **All attention-required notifications**–Displays all attention-required notifications, regardless of their category.
   - **Critical**–Displays notifications in the **Critical** category.
   - **Warning**–Displays notifications in the **Warning** category.
   - **Info**–Displays notifications in the **Info** category.
4. To show only unread notifications, turn on the **Show unread only** toggle.
5. In the notifications list, click a notification to view its message. The full notification is displayed in the details pane on the right.

   When you view a notification, it is automatically marked as read.
6. To mark notifications as read manually, do one of the following:

   - To mark a notification as read, select it in the notifications list, and then click the **Mark as read** button.
   - To mark all notifications as read, click the **Mark all as read** button.
7. If necessary, you can mark a notification as unread by selecting it in the notifications list and clicking the **Mark as unread** button.

Attention-required notifications are reviewed.

# Viewing system notifications

System notifications inform you about events related to Web Console and managed devices. System notifications are grouped by types and get one of the following severity levels: **Critical**, **Warning**, **Info**, or **Success**.

You can view system notifications in one of the following ways:

- In the drop-down panel
- In Notification center

*To view system notifications in the drop-down panel:*

1. At the top of Web Console, click the notification icon ( ).

   The **Notifications** drop-down panel opens.

2. On the **System** tab, view unread notifications.
3. If necessary, mark system notifications as read in one of the following ways:

   - To mark a notification as read, click the close icon ( × ) next to the notification.
   - To mark all notifications as read, click **Mark all as read**.

   After you review all system notifications and mark them as read, the **Notifications** drop-down panel displays a message indicating that there are no new notifications. You can view all system notifications, including both read and unread notifications, in Notification center.

*To view system notifications in Notification center:*

1. At the top of Web Console, click the notification icon ( ).
2. In the **Notifications** drop-down panel that opens, click the **Go to Notification center** button.

   The **Notification center** window opens.

3. On the **System** tab, select one of the following sections:

   - **All system notifications**
   - **Deployment**
   - **Devices**
   - **Protection**
   - **Updates**
   - **Exploit Prevention**
   - **Administration Server**

4. To show only unread notifications, turn on the **Show unread only** toggle.
5. In the notifications list, click a notification to view its message. The full notification is displayed in the details pane on the right.

   When you view a notification, it is automatically marked as read.

6. To mark notifications as read manually, do one of the following:

   - To mark a notification as read, select it in the notifications list, and then click the **Mark as read** button.
   - To mark all notifications as read, click the **Mark all as read** button.

7. If necessary, you can mark a notification as unread by selecting it in the notifications list and clicking the **Mark as unread** button.

System notifications are reviewed.

# Viewing announcements

Announcements are a type of notification that provide information about your version of Kaspersky Security Center Linux and the Kaspersky applications installed on your managed devices. Only announcements relevant to the currently connected Administration Server and the Kaspersky applications installed on the managed devices of this Administration Server are displayed. Announcements are displayed separately for each Administration Server, whether it is primary, secondary, or virtual.

If several administrators use Kaspersky Security Center Linux and they set different interface languages, Kaspersky Security Center Linux displays Kaspersky announcements in every language used by the administrators. When you change the interface language, Kaspersky announcements in the selected language are added to the section automatically after you sign out of the Web Console and then sign in again.

Announcements include the following types of information:

- Security-related information

  Security-related announcements includes critical updates, vulnerability fixes, and recommendations for resolving issues in Kaspersky applications. Security-related announcements are enabled by default. If you do not want to receive the security-related announcements, you can disable this feature.

  You cannot disable the security-related announcements in the trial mode of Kaspersky Security Center Linux.

  To provide information relevant to your network protection configuration, Kaspersky Security Center Linux sends data to Kaspersky cloud servers and receives only announcements related to the Kaspersky applications installed in your network. The data that can be sent to the servers is described in the End User License Agreement that you accept when installing Kaspersky Security Center Linux.

- Marketing information

  Marketing announcements includes special offers, product news, and advertisements related to Kaspersky applications. Marketing announcements are available only if Kaspersky Security Network (KSN) is enabled. You can disable marketing announcements by disabling KSN.

  To provide information that may help you protect your network devices and perform everyday tasks, Kaspersky Security Center Linux sends data to Kaspersky cloud servers and receives relevant announcements. The data that can be sent to the servers is described in the Processed Data section of the KSN Statement.

The announcements get one of the following severity levels: **Critical**, **Warning**, **Info**, or **Success**.

You can view announcements in one of the following ways:

- In the drop-down panel
- In Notification center

*To view announcements in the drop-down panel:*

1. At the top of Web Console, click the notification icon ( ).

   The **Notifications** drop-down panel opens.

2. On the **Announcements** tab, view unread notifications.
3. If necessary, mark notifications as read in one of the following ways:

   - To mark a notification as read, click the close icon ( × ) next to the notification.
   - To mark all notifications as read, click **Mark all as read**.

   After you review all notifications and mark them as read, the **Notifications** drop-down panel displays a message indicating that there are no new notifications. You can view all notifications, including both read and unread notifications, in Notification center.

*To view announcements in Notification center:*

1. At the top of Web Console, click the notification icon ( ).
2. In the **Notifications** drop-down panel that opens, click the **Go to Notification center** button.

   The **Notification center** window opens.

3. On the **Announcements** tab, select one of the following sections:

   - **All announcements**–Displays all notifications, regardless of their category.
   - **Critical**–Displays notifications in the **Critical** category.
   - **Warning**–Displays notifications in the **Warning** category.
   - **Info**–Displays notifications in the **Info** category.

4. To show only unread notifications, turn on the **Show unread only** toggle.
5. In the notifications list, click a notification to view its message. The full notification is displayed in the details pane on the right.

   When you view a notification, it is automatically marked as read.

6. To mark notifications as read manually, do one of the following:

   - To mark a notification as read, select it in the notifications list, and then click the **Mark as read** button.
   - To mark all notifications as read, click the **Mark all as read** button.

7. If necessary, you can mark a notification as unread by selecting it in the notifications list and clicking the **Mark as unread** button.

Announcements are reviewed.

# Disabling Kaspersky announcements

The Kaspersky announcements section (**Monitoring → Kaspersky announcements**) keeps you informed by providing information related to your version of Kaspersky Security Center Linux and managed applications installed on the managed devices. If you do not want to receive Kaspersky announcements, you can disable this feature.

The Kaspersky announcements include two types of information: security-related announcements and marketing announcements.

*To disable security-related announcements:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Kaspersky announcements** section.
3. Switch the toggle button to the **Security-related announcements are disabled** position.
4. Click the **Save** button.

   Kaspersky announcements are disabled.

Marketing announcements are disabled by default. You receive marketing announcements only if you enabled Kaspersky Security Network (KSN). You can disable this type of announcement by disabling KSN.

Disabling KSN may affect managed Kaspersky applications that use KSN services. Such applications may no longer be able to communicate with Kaspersky to send or receive reputation data, telemetry, or statistics.

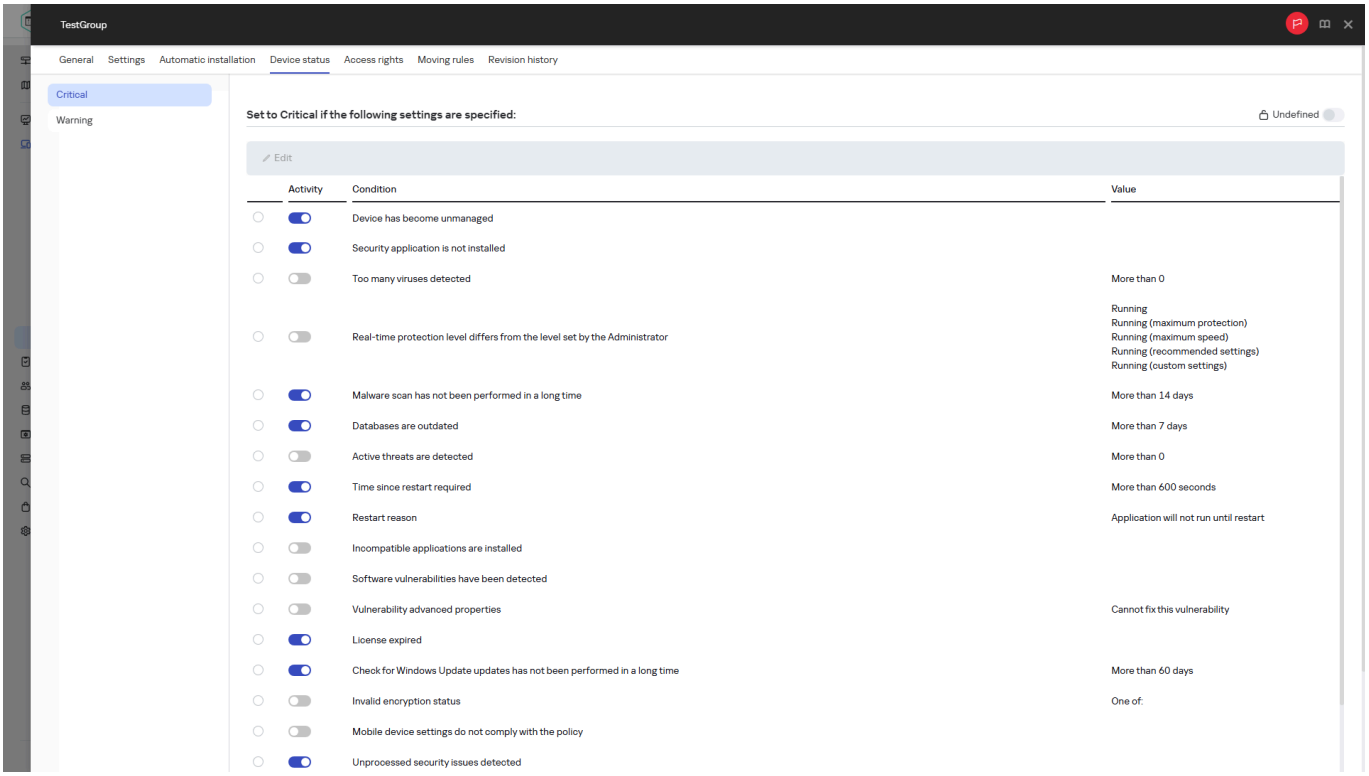
# Configuring the switching of device statuses

You can change conditions to assign the *Critical* or *Warning* status to a device.

*To enable changing the device status to Critical:*

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. Go to the properties of the administration group for which you want to change the device statuses in one of the following ways:
   - Click the name of the administration group.
   - Click the **Show hierarchy** button at the top of the page. In the navigation pane that opens, hover the mouse cursor over the name of the required group, and then click the settings icon ( ⚙ ).

   The administration group properties window opens.
3. In the properties window, select the **Device status** tab.
4. In the left pane, select **Critical**.
5. In the right pane, in the **Set to Critical if the following settings are specified** section, enable the condition to switch a device to the *Critical* status.




> You can change only settings that are not locked in the parent policy.

6. Select the radio button next to the condition in the list.
7. In the upper-left corner of the list, click the **Edit** button.
8. Set the required value for the selected condition.

   Values cannot be set for every condition.

9. Click **OK**.
10. Click **Save** to save changes.

When specified conditions are met, the managed device is assigned the *Critical* status.

*To enable changing the device status to Warning:*

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. In the list of groups that opens, click the link with the name of a group for which you want to change switching the device statuses.
3. In the properties window that opens, select the **Device status** tab.
4. In the left pane, select **Warning**.
5. In the right pane, in the **Set to Warning if the following settings are specified** section, enable the condition to switch a device to the *Warning* status.

   You can change only settings that are not locked in the parent policy.

6. Select the radio button next to the condition in the list.
7. In the upper-left corner of the list, click the **Edit** button.
8. Set the required value for the selected condition.

   Values cannot be set for every condition.
9. Click **OK**.
10. Click **Save** to save changes.

When specified conditions are met, the managed device is assigned the *Warning* status.

# Configuring notification delivery

You can configure notification about events occurring in Kaspersky Security Center Linux. Depending on the notification method chosen, the following types of notifications are available:

- Email—When an event occurs, Kaspersky Security Center Linux sends a notification to the email addresses specified.
- SMS—When an event occurs, Kaspersky Security Center Linux sends a notification to the phone numbers specified.
- Executable file—When an event occurs, the executable file is run on the Administration Server.

*To configure notification delivery of events occurring in Kaspersky Security Center Linux:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens with the **General** tab selected.

2. Click the **Notification** section, and in the right pane select the tab for the notification method you want:

   - **Email**

     The **Email** tab allows you to configure event notification by email.

     In the **SMTP servers** field, specify mail server addresses, separating them with semicolons. You can use the following values:

     - IPv4 or IPv6 address
     - DNS name of the SMTP server

     In the **SMTP server port** field, specify the number of an SMTP server communication port. The default port number is 25.

     If you enable the **Use DNS MX lookup** option, you can use several MX records of the IP addresses for the same DNS name of the SMTP server. The same DNS name may have several MX records with different values of priority of receiving email messages. Administration Server attempts to send email notifications to the SMTP server in ascending order of MX records priority.

     If you enable the **Use DNS MX lookup** option and do not enable usage of TLS settings, we recommend that you use the DNSSEC settings on your server device as an additional measure of protection for sending email notifications.

     If the **Use ESMTP authentication** option is enabled, you can specify the ESMTP authentication settings in the **User name** and **Password** fields. By default, the option is disabled, and the ESMTP authentication settings are not available.

     You can specify TLS settings of connection with an SMTP server:

     - **Do not use TLS**

     You can select this option if you want to disable encryption of email messages.

     - **Use TLS if supported by the SMTP server**

     You can select this option if you want to use a TLS connection to an SMTP server. If the SMTP server does not support TLS, Administration Server connects the SMTP server without using TLS.

     - **Always use TLS, check server certificate validity**

     You can select this option if you want to use TLS authentication settings. If the SMTP server does not support TLS, Administration Server cannot connect the SMTP server.

     We recommend that you use this option for better protection of the connection with an SMTP server. If you select this option, you can set authentication settings for a TLS connection.

     If you select **Always use TLS, check server certificate validity** value, you can specify a certificate for authentication of the SMTP server and choose whether you want to enable communication through any version of TLS or only through TLS 1.2 or later versions. Also, you can specify a certificate for client authentication on the SMTP server.

     You can specify certificates for a TLS connection by clicking the **Specify certificates** link:

     - Browse for an SMTP server certificate file:

You can receive a file with the list of certificates from a trusted certification authority and upload the file to Administration Server. Kaspersky Security Center Linux checks whether the certificate of an SMTP server is also signed by a trusted certification authority. Kaspersky Security Center Linux cannot connect to an SMTP server if the certificate of the SMTP server is not received from a trusted certification authority.

- Browse for a client certificate file:

You can use a certificate that you received from any source, for example, from any trusted CA. You must specify the certificate and its private key by using one of the following certificate types:

- X-509 certificate:

You must specify a file with the certificate and a file with the private key. The two files are independent of each other. The order in which the files are loaded does not matter. When both files are loaded, you must specify the password for decoding the private key. The password can have an empty value if the private key is not encoded.

- pkcs12 container:

You must upload a single file that contains the certificate and its private key. When the file is loaded, you must then specify the password for decoding the private key. The password can have an empty value if the private key is not encoded.

Clicking the **Send test message** button allows you to check whether you configured notifications properly: the application sends a test notification to the email addresses that you specified.

In the **Recipients (email addresses)** field, specify the email addresses to which the application will send notifications. You can specify multiple addresses in this field, by separating them with semicolons.

In the **Subject** field, enter the email subject using substitution parameters, for example: `[KSC-SAMARA-1] [%SEVERITY%] %EVENT%`. Example of what the subject line looks like in case of a detected threat: `[KSC-SAMARA-1] [Critical] Threat detected`. You can leave this field empty.

In the **Subject template** drop-down list, select the template for your subject. A variable determined by the selected template is placed automatically in the **Subject** field. You can construct an email subject selecting several subject templates.

In the **Sender email address: If this setting is not specified, the recipient address will be used instead. Warning: We do not recommend using a fictitious email address** field, specify the sender email address. If you leave this field empty, by default, the recipient address is used. It is not recommended to use fictitious email addresses.

The **Notification message** field contains standard text with information about the event that the application sends when an event occurs. This text includes substitute parameters, such as event name, device name, and domain name. You can edit the message text by adding other substitute parameters with more relevant details about the event.

**Example of field value**

```
Sender - KSC-SAMARA-1

Host: %COMPUTER%

Product: %KL_PRODUCT%

Version: %KL_VERSION%

Occurred at: %RISE_TIME%

Event: %EVENT%

Details:
```

%DESCR%

The Sender string is optional. For example, if you have multiple Administration Servers, you can specify the name of the Administration Server from which the notification was received: Sender - KSC-SAMARA-1.

**Example of what the notification text looks like:**

```
Sender - KSC-SAMARA-1

Host: nb-123456.example.net

Product: Kaspersky Endpoint Security 12.5 for Linux

Version: 12.5.0.1569

Occurred at: 2026-08-17T13:15:36

Event: Threat detected

Details:

Initiator: Product; Task type: ODS; ID of running task: 107; User receiving access:
root; Object type: File; File owner: user; Detection certainty: Sure; File:
/home/user/eicar_com.zip//eicar.com; Detected object name: EICAR-Test-File; Detected
object type: Virware; MD5 hash: <hash>; Unique ID: <ID>
```

If the notification text contains a percent sign (%), you have to type it twice in a row to allow message sending. For example, "CPU load is 100%%".

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send during the specified time interval.

- **SMS**

The **SMS** tab allows you to configure the transmission of SMS notifications about various events to a cell phone. SMS messages are sent through a mail gateway.

In the **SMTP servers** field, specify mail server addresses, separating them with semicolons. You can use the following values:

- IPv4 or IPv6 address
- Windows network name (NetBIOS name) of the device
- DNS name of the SMTP server

In the **SMTP server port** field, specify the number of an SMTP server communication port. The default port number is 25.

If the **Use ESMTP authentication** option is enabled, you can specify the ESMTP authentication settings in the **User name** and **Password** fields. By default, the option is disabled, and the ESMTP authentication settings are not available.

You can specify TLS settings of connection with an SMTP server:

- **Do not use TLS**

You can select this option if you want to disable encryption of email messages.

- **Use TLS if supported by the SMTP server**

You can select this option if you want to use a TLS connection to an SMTP server. If the SMTP server does not support TLS, Administration Server connects the SMTP server without using TLS.

- **Always use TLS, check server certificate validity**

You can select this option if you want to use TLS authentication settings. If the SMTP server does not support TLS, Administration Server cannot connect the SMTP server.

> We recommend that you use this option for better protection of the connection with an SMTP server. If you select this option, you can set authentication settings for a TLS connection.

If you select **Always use TLS, check server certificate validity** value, you can specify a certificate for authentication of the SMTP server and choose whether you want to enable communication through any version of TLS or only through TLS 1.2 or later versions. Also, you can specify a certificate for client authentication on the SMTP server.

You can specify SMTP server certificate file by clicking the **Specify certificates** link:

You can receive a file with the list of certificates from a trusted certification authority and upload the file to Administration Server. Kaspersky Security Center Linux checks whether the certificate of an SMTP server is also signed by a trusted certification authority. Kaspersky Security Center Linux cannot connect to an SMTP server if the certificate of the SMTP server is not received from a trusted certification authority.

In the **Recipients (email addresses)** field, specify the email addresses to which the application will send notifications. You can specify multiple addresses in this field, by separating them with semicolons. The notifications will be delivered to the phone numbers associated with the specified email addresses.

In the **Subject** field, specify the email subject.

In the **Subject template** drop-down list, select the template for your subject. A variable according to the selected template is put in the **Subject** field. You can construct an email subject selecting several subject templates.

In the **Sender email address: If this setting is not specified, the recipient address will be used instead. Warning: We do not recommend using a fictitious email address** field, specify the sender email address. If you leave this field empty, by default, the recipient address is used. It is not recommended to use fictitious email addresses.

In the **Phone numbers of SMS message recipients** field, specify the cell phone numbers of the SMS notification recipients.

In the **Notification message** field, specify a text with information about the event that the application sends when an event occurs. This text can include substitute parameters, such as event name, device name, and domain name.

> If the notification text contains a percent sign (%), you have to type it twice in a row to allow message sending. For example, "CPU load is 100%%".

Click the **Configure numeric limit of notifications** link to specify the maximum number of notifications that the application can send during the specified time interval.

Click the **Send test message** to check whether you configured notifications properly: the application sends a test notification to the recipient that you specified.

- **Executable file to be run**

The executable file must contain the environment variables of the event that you want the administrator to receive.

In the **Executable file to be run on the Administration Server when an event occurs** field, specify the folder and the name of the file to be run.

Example of field value:

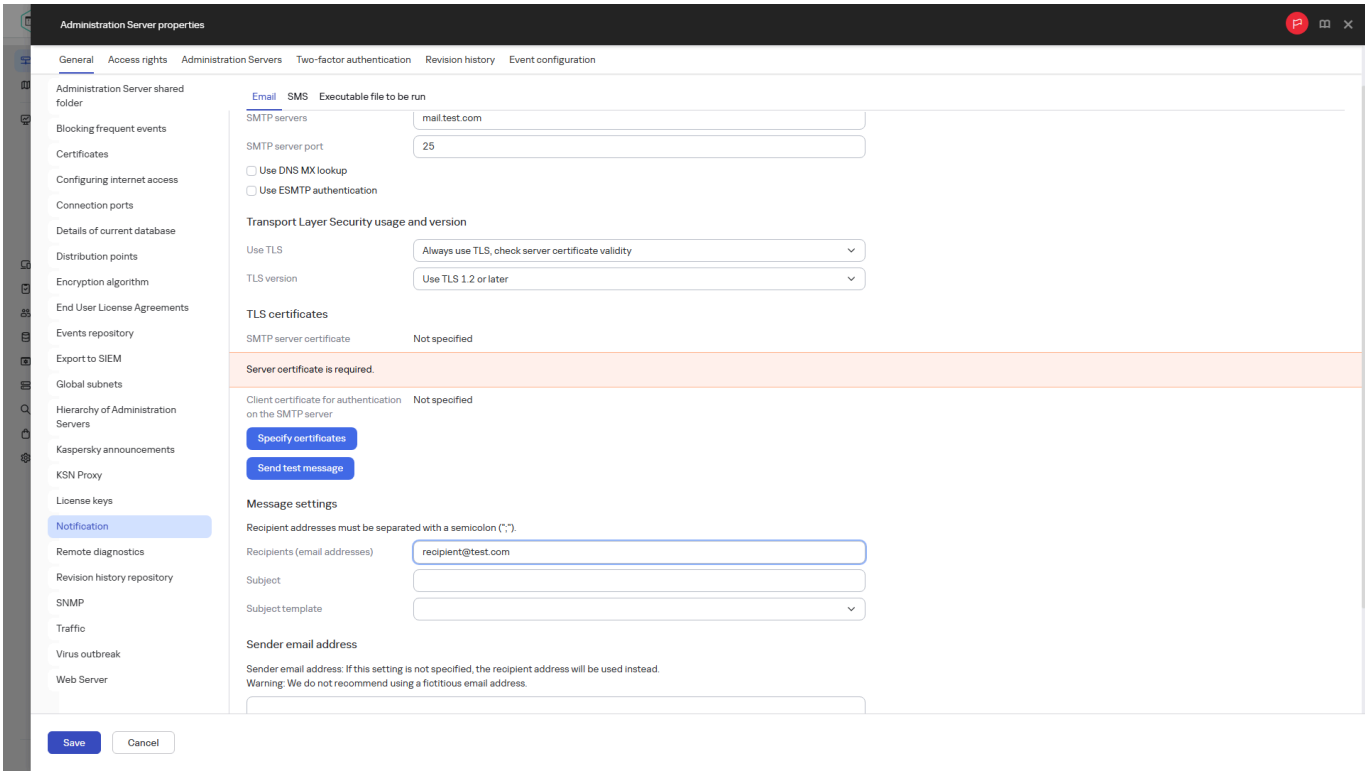
```
/opt/scripts/notifications.sh
```

The file must be prepared in advance by specifying substitution parameters that stand for the event information that will be sent in the message. The folder and the file must be located on the Administration Server.

Example of script for testing or debugging:

```
#!/usr/bin/env bash
touch /tmp/ksc_notification.txt
echo "$RISE_TIME $COMPUTER $EVENT" >> /tmp/ksc_notification.txt
```

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send during the specified time interval.




Selecting the notification method

3. On the tab, define the notification settings.

4. Click **Save** to save the changes and close the Administration Server properties window.

The saved notification delivery settings are applied to all events that occur in Kaspersky Security Center Linux.

You can override notification delivery settings for certain events in the **Event configuration** section of the Administration Server settings, of a policy's settings, or of an application's settings.

# Testing notifications

To check whether event notifications are sent, the application uses the notification of the EICAR test virus detection on client devices.

*To verify sending of event notifications:*

1. Stop the real-time file system protection task on a client device and copy the EICAR test virus to that client device. Then, re-enable real-time protection of the file system.

2. Run a scan task for client devices in an administration group or for specific devices, including one with the EICAR test virus.

   If the scan task is configured correctly, the test virus will be detected. If notifications are configured correctly, you are notified that a virus has been detected.

*To open a record of the test virus detection:*

1. In the main menu, go to **Monitoring** → **Event selections**.

2. Click the **Recent events** selection name.

   In the window that opens, the notification about the test virus is displayed.

The EICAR test virus contains no code that can do harm to your device. However, most manufacturers' security applications identify this file as a virus. You can download the test virus from the official EICAR website.

# About device statuses

Kaspersky Security Center Linux assigns a status to each managed device. The particular status depends on whether the conditions defined by the user are met. In some cases, when assigning a status to a device, Kaspersky Security Center Linux takes into consideration the device's visibility flag on the network (see the table below). For example, if a managed device was assigned the *Critical* status because the *Databases are outdated* condition was met, and later the visibility flag was set for the device, then the device is assigned the *OK* status. If Kaspersky Security Center Linux does not find a device on the network within two hours, the visibility flag of the device is set to *Not Visible*.

The statuses are the following:

- *Critical* or *Critical/Visible*
- *Warning* or *Warning/Visible*
- *OK* or *OK/Visible*

The table below lists the default conditions that must be met to assign the *Critical* or *Warning* status to a device, with all possible values.

Conditions for assigning a status to a device

| Condition | Condition description | Available values |
|---|---|---|
| Security application is not installed | Network Agent is installed on the device, but a security application is not installed. | • Toggle button is on<br>• Toggle button is off |

| Condition | Condition description | Available values |
|---|---|---|
| Too many viruses detected | Some viruses have been found on the device by a task for virus detection, for example, the Malware scan task, and the number of viruses found exceeds the specified value. | More than 0 |
| Real-time protection level differs from the level set by the Administrator | The device is visible on the network, but the real-time protection level differs from the level set (in the condition) by the administrator for the device status. | • Stopped<br>• Suspended<br>• Running |
| Malware scan has not been performed in a long time | The device is visible on the network and a security application is installed on the device, but neither the *Malware scan* task nor a local scan task has been run within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 7 days ago or earlier. | More than 1 day |
| Databases are outdated | The device is visible on the network and a security application is installed on the device, but the anti-virus databases have not been updated on this device within the specified time interval. The condition is applicable only to devices that were added to the Administration Server database 1 day ago or earlier. | More than 1 day |
| Not connected in a long time | Network Agent is installed on the device, but the device has not connected to an Administration Server within the specified time interval, because the device was turned off. | More than 1 day |
| Active threats are detected | The number of unprocessed objects in the **Active threats** folder exceeds the specified value. | More than 0 items |
| Time since restart required | The device is visible on the network, but a restart has been required by an application for longer than the specified time interval. | More than 0 minutes |
| Restart reason | The device is visible on the network, but an application requires a device restart for one of the selected reasons. | • Unknown reason<br>• Application will not run until restart<br>• Restart is required to complete update; application is running<br>• Restart is required to launch update<br>• Restart is required to complete scan or disinfection<br>• Restart is required to complete remote installation/uninstallation<br>• Completing data encryption on disk |
| Incompatible applications are installed | The device is visible on the network, but software inventory performed through Network Agent has detected incompatible applications installed on the device. | • Toggle button is off<br>• Toggle button is on |
| Software vulnerabilities have been detected | The device is visible on the network and Network Agent is installed on the device, but the *Find vulnerabilities and required updates* task has detected vulnerabilities with the specified severity level in applications installed on the device. | • Critical<br>• High<br>• Medium<br>• Ignore if the vulnerability cannot be fixed<br>• Ignore if an update is assigned for installation |
| License expired | The device is visible on the network, but the license has expired. | • Toggle button is off<br>• Toggle button is on |
| License expires soon | The device is visible on the network, but the license will expire on the device in less than the specified number of days. | More than 0 days. |

| Condition | Condition description | Available values |
|---|---|---|
| Check for Windows Update updates has not been performed in a long time | The device is visible on the network, but the *Find vulnerabilities and required updates* task has not been run within the specified time interval. | More than 1 day |
| Invalid encryption status | Network Agent is installed on the device, but the device encryption result is equal to the specified value. | • Does not comply with the policy due to the user's refusal (for external devices only)<br>• Does not comply with the policy due to an error<br>• Restart is required when applying the policy<br>• No encryption policy is specified<br>• Not supported<br>• When applying the policy |
| Mobile device settings do not comply with the policy | The mobile device settings are other than the settings that were specified in the Kaspersky Endpoint Security for Android policy during the check of compliance rules. | • Toggle button is off<br>• Toggle button is on |
| Unprocessed security issues detected | Some unprocessed security issues have been found on the device. Security issues can be created either automatically, through managed Kaspersky applications installed on the client device, or manually by the administrator. | • Toggle button is off<br>• Toggle button is on |
| Device status defined by application | The status of the device is defined by the managed application.<br>Managed devices can have a status defined by managed applications regardless of Kaspersky Security Center Linux settings. After this status returns one of the statuses defined by Kaspersky Security Center Linux, Administration Server assigns to a managed device the most critical status of those returned by the managed application and assigned by Administration Server. Statuses defined by managed applications have descriptions transferred by managed applications. You can view the descriptions in the list of managed devices, **Status description** column. | • Toggle button is off<br>• Toggle button is on |
| Device is out of disk space | Free disk space on the device is less than the specified value, or the device could not be synchronized with the Administration Server. The *Critical* or *Warning* status is changed to the *OK* status when the device is successfully synchronized with the Administration Server and free space on the device is greater than or equal to the specified value. | More than 0 MB |
| Device has become unmanaged | During device discovery, the device was recognized as visible on the network, but more than three attempts to synchronize with the Administration Server failed. | • Toggle button is off<br>• Toggle button is on |
| Protection is disabled | The device is visible on the network, but the security application on the device has been disabled for longer than the specified time interval.<br>In this case, the state of the security application is *stopped* or *failure*, and differs from the following: *starting*, *running*, or *suspended*. | More than 0 minutes |
| Security application is not running | The device is visible on the network and a security application is installed on the device but is not running. | • Toggle button is off<br>• Toggle button is on |

Kaspersky Security Center Linux allows you to set up automatic switching of the status of a device in an administration group when specified conditions are met. When the specified conditions are met, the client device is assigned one of the following statuses: *Critical* or *Warning*. When the specified conditions are not met, the client device is assigned the *OK* status.

Different statuses may correspond to different values of one condition. For example, by default, if the **Databases are outdated** condition has the **More than 3 days** value, the client device is assigned the *Warning* status; if the value is **More than 7 days**, the *Critical* status is assigned.

If you upgrade Kaspersky Security Center Linux from the previous version, the values of the **Databases are outdated** condition for assigning the status to *Critical* or *Warning* do not change.

# Parameters and environment variables for describing an event

When configuring notifications about Kaspersky Security Center Linux events, you can use parameters and environment variables to describe the events (see the table below).

If you have chosen to run an executable file as a notification method, use variables when writing the file.

If you want to send notifications about events by email or SMS, when configuring notifications on the corresponding tab, you can also specify variables in the **Subject** and **Notification message** fields.

Parameters and environment variables for describing an event

| Substitution parameter (for use in notifications) | Environment variable (for use in scripts) | Environment variable description |
|---|---|---|
| %SEVERITY% | $SEVERITY | Event severity. Possible values:<br>• **Info**<br>• **Warning**<br>• **Error**<br>• **Critical** |
| %COMPUTER% | $COMPUTER | Name of the device where the event occurred.<br>Maximum length of the device name is 256 characters. |
| %DOMAIN% | $DOMAIN | Domain name of the device where the event occurred. |
| %EVENT% | $EVENT | Name of the event type.<br>Maximum length of the event type name is 50 characters. |
| %DESCR% | $DESCR | Event description.<br>Maximum length of the description is 1000 characters. |
| %RISE_TIME% | $RISE_TIME | Event creation time. |
| %KLCSAK_EVENT_TASK_DISPLAY_NAME% | $KLCSAK_EVENT_TASK_DISPLAY_NAME | Task name.<br>Maximum length of the task name is 100 characters. |
| %KL_PRODUCT% | $KL_PRODUCT | Application name. |
| %KL_VERSION% | $KL_VERSION | Application version number. |
| %$KLCSAK_EVENT_SEVERITY_NUM% | $KLCSAK_EVENT_SEVERITY_NUM | Event severity number. Possible values:<br>• 1—**Info**<br>• 2—**Warning**<br>• 3—**Error**<br>• 4—**Critical** |
| %HOST_IP% | $HOST_IP | IP address of the device where the event occurred. |
| %HOST_CONN_IP% | $HOST_CONN_IP | Connection IP address of the device where the event occurred. |

# Viewing information about the detects of threats

You can enable or disable displaying information about alerts.

After you activate Administration Server under a Kaspersky Extended Detection and Response Optimum license or under a Kaspersky Next XDR Optimum license, Kaspersky Security Center Web Console automatically displays the **Alerts** subsection in the **Monitoring** section of the main menu.

*To enable or disable displaying the **Alerts** section in the main menu:*

1. In the main menu, go to **Settings** → **Interface options**.
2. Enable or disable the **Show EDR alerts** option.
3. Click **Save**.

When the **Show EDR alerts** option is enabled, the console displays the **Alerts** subsection in the **Monitoring** section of the main menu. In the **Alerts** subsection, you can view information about the detects of threats on the endpoint devices.

Also, you can add a widget that displays information about alerts.

To display detailed information about detected threats in the alert card correctly, you have to install the Kaspersky Endpoint Agent plug-in and the compatible version of the Kaspersky Endpoint Security plug-in (Kaspersky Endpoint Security for Linux 12.1 or later, Kaspersky Endpoint Security for Mac 12.1 or later, or Kaspersky Endpoint Security for Windows 12.6 or later).

Use the **Filter** menu to filter alerts by date and field values.

The **Object type** field contains the following values:

- unknown
- Phishing link
- virus
- Trojan
- malicious tool
- backdoor
- worm
- other application
- Adware
- Pornware
- Dangerous packed program
- Dangerous behavior

The **Automatic response** field contains the following values:

- Malicious object detected
- Object deleted

- Object disinfected
- Object failed to disinfect
- Object moved to Quarantine
- Password-protected archive detected
- Virus detected

# Integrations for responding to alerts

If you have the Kaspersky Next XDR Optimum license, you can configure integrations with the following solutions for responding to threats:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

These integrations are available if you activated Administration Server under a Kaspersky Next XDR Optimum license.
To perform response actions, you have to deploy the Kaspersky Next XDR Optimum license key to your managed applications.
When using the Kaspersky Next XDR Optimum functionality under a trial license, you must first add a secondary physical Administration Server, activate this secondary Administration Server under the trial license, and then deploy the license key to your devices managed by this Administration Server.

If you are using the Kaspersky Next EDR Optimum license, you do not have to activate the applications installed on your managed devices under the Kaspersky Next XDR Optimum license. You must do it only for new devices, if any.

Because the Kaspersky Next XDR Optimum license supports multitenancy, you can centrally distribute the license key to managed applications. Automatic distribution of the license to secondary and virtual Administration Servers is not supported.

To configure the integrations, you must have the **Read** and **Write** rights for the **General features: Application integration** functional area.

# Configuring integration with Active Directory for performing response actions

Integration with Active Directory enables you to perform response actions for Active Directory users affected by or involved in the alert.

To configure the integration with Active Directory for responding to alerts, you must use Kaspersky Security Center Linux Administration Server version 15.4 or later.

The integration with Active Directory for responding to alerts, and the settings for scanning the Active Directory domain controller (the address and user credentials of the domain controller) you specify when configuring a domain controller polling, are two different settings. Since you need to ensure that the user for whom a response action is to be performed has an Active Directory account, you must configure both the integrations: for scanning and for responding. The order is not significant.

The integration settings are not inherited and are applied only to the Administration Server (physical or virtual) on which you configure these settings.

*To configure integration with Active Directory for responding to alerts:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens with the **General** tab selected.

2. Do one of the following:

   - Select the **Distribution points** section, click the name of the required distribution point, and then in the properties window that opens, select the **Active Directory** section.
   - Select the **Active Directory response** section.

3. In the right pane, enable the **Active Directory integration** toggle switch.

   Later, if you want to turn off the integration, you can only do it for all connections by disabling the **Active Directory integration** toggle switch. You cannot turn off the integration for a separate connection. Instead, you can delete the connection.

   > When you enable or disable the **Active Directory integration** toggle switch, the setting is applied for both the **Active Directory response** and the **Distribution points** sections.

4. Create a connection to the Active Directory domain controller by clicking the **Add** button.

5. In the window that opens, specify the following parameters for the connection:

   - **Domain controller address**

     Computer name, for example: `server.mycompany.com`.

     You can specify several addresses. All domain controllers whose addresses you specify must belong to the same domain.

   - **Active Directory domain name**

     DNS fully qualified domain name, for example: `mycompany.com`

     Also, you can specify SAM or NetBIOS name, for example: `mycompany`

     Use lowercase letters. If you create several connections for the Administration Server or a distribution point, specify different names for each connection.

     > To perform response actions, the Active Directory domain name that you specify in this field must match the Active Directory domain name specified in the alert.

   - **Login**

     Login of the Active Directory account with administrator rights under which the response actions are to be performed.

- **Password**

  Password of the Active Directory account with administrator rights under which the response actions are to be performed.

6. If you want to check the connection status, click the **Check connection** button.

   If the connection is successfully established, the **Connected** status is displayed. Otherwise, the status is **Failed**, and an error message is displayed with the domain controllers to which you failed to connect.

   You must take into account how the connection to Active Directory is made: **from a Linux device or from a Windows device**.

### Connecting from a Linux device

By default, when connecting and authenticating to a domain controller from a Linux device, the logic is the following:

1. Administration Server or a distribution point attempts to connect to the domain controller over LDAPS.

   The strong verification of the LDAP server certificate is performed.

2. You place the public part of the domain controller certificate into the system certificate repository to validate the certificate.

   The OS-dependent path to the system certificate authority (CA) is used to access the certificate chain.

   For example:

   - /etc/ssl/certs/ca-certificates.crt—Path for Debian-based operating systems (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem—Path for CentOS or Red Hat.

3. If the LDAPS connection fails, an error occurs, and no other connection protocol is used.

   In case of issues with LDAPS, you can contact Kaspersky Technical Support.

If you do not want to install the certificate into the system certificate repository, you can use the KLNAG_LDAP_SSL_CACERT flag to set the path to the domain controller certificate. To do it, run the command:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

where `</path/to/domain-controller/cert>` is the path to the public part of the domain controller certificate.

For example, if the path is `"/var/opt/kaspersky/ldap_cert.crt"`, the command is `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Connecting from a Windows device

When connecting and authenticating to a domain controller from a Windows device, the connection settings are defined by the domain.

You only have to ensure that:

- LDAPS is enabled and port 636 is available on the device.
- You allow connections to the domain controller through a firewall or a proxy server.

7. Click **Save**.

The window is closed, and the connection is displayed in the table of connections.

In the table of connections, you can do the following:

- Edit connection parameters.

  To do this, click the link with the **Domain controller address** parameter for the required connection. In the window that opens, change the required settings, and then click the **Save** button.

  You can edit only the **Login** and **Password** parameters.

- Delete connections.

  To do this, select the check box next to the connection you want to delete, click the **Remove** button in the toolbar, and then confirm the deletion of the connection.

# Configuring integration with Kaspersky Automated Security Awareness Platform

Integration with Kaspersky Automated Security Awareness Platform (hereinafter also referred to as KASAP) enables you to assign KASAP learning courses to users who are associated with alerts.

The integration settings are not inherited and are applied only to the Administration Server (physical or virtual) on which you configure these settings.

Before configuring an integration in Kaspersky Security Center Web Console, you have to create an authorization token and obtain a URL for API requests in KASAP.

*To configure integration with Kaspersky Automated Security Awareness Platform:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens with the **General** tab selected.

2. Select the **KASAP** section.

3. In the right pane, enable the **KASAP integration** toggle switch.

4. Specify the settings to be used for connection to KASAP:

   - **API token**—Token that you created to access KASAP Open API.
   - **URL**—URL for API requests that you obtained when creating the API token.
   - **Use a proxy server**—Toggle switch that enables the use of a proxy server when connecting to KASAP.
     The toggle switch is turned off by default.

5. If necessary, verify the settings you specified by clicking the **Check connection** button.
   The connection status is displayed.

6. Click the **Save** button.

The integration with Kaspersky Automated Security Awareness Platform is configured.

After the KASAP integration settings are saved, you can view the list of KASAP learning groups by clicking the **View groups** button.

If necessary, when the group list is displayed, you can update it by clicking the **Refresh groups** button.

> You cannot hide the list after you open it. If you disable the **KASAP integration** toggle switch, the list of KASAP groups is not displayed.

# Configuring integration with Kaspersky Threat Intelligence Portal Sandbox

Integration with Kaspersky Threat Intelligence Portal (hereinafter also referred to as Kaspersky TIP) enables you to execute the files moved to the **Quarantine** section by using Kaspersky Sandbox—a safe environment isolated from your corporate network.

The integration settings are not inherited and are applied only to the Administration Server (physical or virtual) on which you configure these settings.

> Before configuring integration, you have to obtain an authorization token for API requests on Kaspersky TIP.

*To configure integration with Kaspersky TIP Sandbox:*

1. In the main menu, click the Administration Server name.
   The Administration Server properties window opens with the **General** tab selected.

2. Select **Kaspersky TIP**.

3. In the right pane, enable the **Integration** toggle switch.
   The settings for connection to Kaspersky TIP are displayed.

If after configuring and saving the integration settings you disable the **Integration** toggle switch, the settings are not deleted but the response cannot be performed.

4. Click the **Add token** button, and in the displayed window, specify the token previously obtained from Kaspersky TIP, then click the **Add** button.

   The window closes, and the API token is added.

5. If you want to use a proxy server when connecting to Kaspersky TIP, enable the **Use a proxy server** toggle switch.

   The toggle switch is turned off by default.

6. Click the **Save** button.

The integration with Kaspersky TIP Sandbox is configured.

Now, you can send files from the **Quarantine** section to Kaspersky TIP Sandbox for threat analysis. Maximum size of a file is 100 MB.

Because the Kaspersky Next XDR Optimum license supports multitenancy, files placed in **Quarantine** are divided by tenants. This tenant-level separation also applies when sending files to the Kaspersky TIP Sandbox and viewing the results if the administrator uses a dedicated TIP account and an API token related to each tenant. However, centralized management of the **Quarantine** section for all tenants is not possible, as the quarantine list does not display objects according to the server hierarchy.

# Grouping alerts by attributes

Alerts aggregation helps identify alerts that may be related to the same incident, simplifying the investigation process.

To enable the functionality of alert aggregation, you have to do the following:

- Enable the **Alerts** subsection in the main menu.
- Activate Administration Server under a Kaspersky Next XDR Optimum license, and then deploy the Kaspersky Next XDR Optimum license key to your managed applications.

  When using a Kaspersky Next XDR Optimum functionality under a trial license in the test mode, you must first add a secondary physical Administration Server, and then activate this server under this license.

If you are using the Kaspersky Next EDR Optimum license, you do not have to activate the applications installed on your managed devices under the Kaspersky Next XDR Optimum license. You must do it only for new devices, if any. Because the Kaspersky Next XDR Optimum license supports multitenancy, you can centrally distribute the license key to managed applications. Automatic distribution of the license to secondary and virtual Administration Servers is not supported.

You can aggregate alerts by device name, account, or hash name (SHA256).

Alerts are aggregated by an attribute only if that attribute is not empty.

Alerts are aggregated together if they share at least one attribute and occur within 24 hours of any other alert in the group.

*To aggregate alerts by attributes:*

1. In the main menu, go to **Monitoring** → **Alerts**.
2. Do one of the following:
   - Enable the **Alerts aggregation** toggle switch, then select one or more attributes to aggregate alerts by:
     - **Device name**
     - **Account**
     - **File hash (SHA256)**

     The **Device name** and **Account** attributes are selected by default.
   - Click the settings icon ( ⚙ ). In the **Table settings** pane that opens, go to the **Grouping** tab. Select **Aggregation group ID** and click **Apply**.

   When aggregation is enabled, alerts are sorted by **Event time** from newest to oldest. Additional sorting options are not supported. Selecting a different grouping option will disable aggregation.

The table displays alerts aggregated by attributes. Unaggregated alerts are displayed at the bottom of the table.

Each alert is assigned to only one group after aggregation.

# Cloud Discovery

Kaspersky Security Center Linux allows you to monitor the use of cloud services on managed devices running Windows and to block access to cloud services that you consider unwanted. Cloud Discovery tracks user attempts to gain access to these services through both browsers and desktop applications. It also tracks user attempts to gain access to cloud services over unencrypted connections (for example, using the HTTP protocol). This feature helps you to detect and halt the use of cloud services by shadow IT.

The blocking capability is available only if you activated Kaspersky Security Center Linux under a Kaspersky Next EDR Optimum or Kaspersky Next XDR Expert license.

The blocking capability is available only if you use Kaspersky Endpoint Security 11.2 for Windows or later. Earlier versions of the security application only allow you to monitor the use of cloud services.

You can enable the Cloud Discovery feature and select the security policies or profiles for which you want to enable the feature. You can also enable or disable the feature separately in each security policy or profile. You can block access to cloud services that you do not want users to access.

To be able to block access to unwanted cloud services, make sure that the following prerequisites are met:

- You use Kaspersky Endpoint Security 11.2 for Windows or later. Earlier versions of the security application only allow you to monitor the use of cloud services.
- You have purchased a Kaspersky Next license tier that includes the ability to block access to unwanted cloud services. For details, refer to Kaspersky Next Help.

The Cloud Discovery widget and the Cloud Discovery reports display information about successful and blocked attempts to gain access to cloud services. The widget also displays the risk level of each cloud service. Kaspersky Security Center Linux gets information about the use of cloud services from all of the managed devices that are protected only by the security profiles that have the feature enabled.

# Enabling Cloud Discovery by using the widget

The Cloud Discovery feature allows you to get information about the use of cloud services from all of the managed devices that are protected only by the security policies that have the feature enabled. You can enable or disable Cloud Discovery for the Kaspersky Endpoint Security for Windows policy only.

There are two ways to enable the Cloud Discovery feature:

- By using the Cloud Discovery widget.
- In the properties of the Kaspersky Endpoint Security for Windows policy.

  For details on how to enable the Cloud Discovery feature in the Kaspersky Endpoint Security for Windows policy properties, refer to the Cloud Discovery section of Kaspersky Endpoint Security for Windows Help.

Note that you can disable the Cloud Discovery feature in the Kaspersky Endpoint Security for Windows policy parameters only.

To enable Cloud Discovery, you must have the **Write** right in the **General features: Basic functionality** functional area.

*To enable the Cloud Discovery feature by using the Cloud Discovery widget:*

1. Go to Kaspersky Security Center Linux.
2. In the main menu, go to **Monitoring** → **Dashboard**.
3. On the **Cloud Discovery** widget, click the **Enable** button.

   If you have Kaspersky Endpoint Security for Windows version 12.4 installed, enable the Cloud Discovery feature in the Kaspersky Endpoint Security for Windows policy properties. For details, refer to the Cloud Discovery section of Kaspersky Endpoint Security for Windows Help.

   If you have Kaspersky Endpoint Security for Windows earlier than version 12.4, update the Kaspersky Endpoint Security for Windows plug-in to version 12.5.

4. In the **Enable Cloud Discovery** window that opens, select the security policies for which you want to enable the feature, and then click the **Enable** button.

   The following policy settings will be enabled automatically: **Inject script into web traffic to interact with web pages**, **Web Session monitor**, and **Encrypted connections scan**.

The Cloud Discovery feature is enabled and the widget is added to the dashboard.

# Adding the Cloud Discovery widget to the dashboard

You can add the **Cloud Discovery** widget to the dashboard to monitor the use of cloud services on managed devices.

To add the Cloud Discovery widget to the dashboard, you must have the **Write** right in the **General features: Basic functionality** functional area.

*To add the Cloud Discovery widget to the dashboard:*

1. Go to Kaspersky Security Center Linux.
2. In the main menu, go to **Monitoring** → **Dashboard**.
3. Click the **Add or restore widget** button.
4. In the list of available widgets, click the chevron icon (>) next to the **Other** category.
5. Select the **Cloud Discovery** widget, and then click the **Add** button.

   If the Cloud Discovery feature is disabled, follow the instructions in the Enabling Cloud Discovery by using the widget section.

The selected widget is added at the end of the dashboard.

# Viewing information about the use of cloud services

You can view the **Cloud Discovery** widget that shows information about attempts to gain access to cloud services. The widget also displays the risk level of each cloud service. Kaspersky Security Center Linux gets information about the use of cloud services from all managed devices that are protected only by the security profiles that have this feature enabled.

Before viewing, make sure that:

- The Cloud Discovery widget is added to the dashboard.
- The Cloud Discovery feature is enabled.
- You have the **Read** right in the **General features: Basic functionality** functional area.

*To view the Cloud Discovery widget:*

1. Go to Kaspersky Security Center Linux.
2. In the main menu, go to the **Monitoring** → **Dashboard**.

   The **Cloud Discovery** widget is displayed on the dashboard.
3. On the left side of the **Cloud Discovery** widget, select a category of cloud services.

   The table on the right side of the widget displays up to five services from the selected category, to which users most often try to gain access. Both successful and blocked attempts are counted.
4. On the right side of the widget, select a specific service.

   The table below displays up to ten devices that most often attempt to gain access to the service. In this table, you can generate two types of reports: report on successful access attempts and report on blocked access attempts.

   In addition, in this table you can block access to the cloud service for a specific device.

The widget displays the requested information.

From the displayed widget, you can do the following:

- Proceed to the **Monitoring** → **Reports** section, to view the Cloud Discovery reports.
- Block or allow access to the selected cloud service.

The blocking capability is available only if you activated Kaspersky Security Center Linux under a Kaspersky Next EDR Optimum or Kaspersky Next XDR Expert license.
The blocking capability is available only if you use Kaspersky Endpoint Security 11.2 for Windows or later. Earlier versions of the security application only allow you to monitor the use of cloud services.

# Risk level of a cloud service

For each cloud service, Cloud Discovery provides you with a risk level. The risk level helps you determine which services do not fit the security requirements of your organization. For example, you may want to take the risk level into account when deciding whether to block access to a certain service.

The risk level is an estimated index and does not say anything about the quality of a cloud service or about the service manufacturer. The risk level is simply a recommendation from Kaspersky experts.

Risk levels of cloud services are displayed in the Cloud Discovery widget and in the list of all monitored cloud services.

# Blocking access to unwanted cloud services

You can block access to cloud services that you do not want users to access. You can also allow access to cloud services that were previously blocked.

Among other considerations, you may want to take the risk level into account when deciding whether to block access to a certain service.

You can block or allow access to cloud services for a security policy or profile.

There are two ways to block access to unwanted cloud services:

- By using the Cloud Discovery widget.

  In this case, you can block access to the services one by one.

- In the properties of the Kaspersky Endpoint Security for Windows policy.

  In this case, you can block access to the services one by one or block an entire category at once.

  For details on how to enable the Cloud Discovery feature in the Kaspersky Endpoint Security for Windows policy properties, refer to the Cloud Discovery section of Kaspersky Endpoint Security for Windows Help.

*To block or allow access to a cloud service by using the widget:*

1. Open the Cloud Discovery widget, and then select the required cloud service.
2. In the **Top 10 devices that use the service** pane, find the security policy or profile for which you want to block or allow the service.
3. On the required line, in the **Access status in policy or profile** column, do any of the following:
   - To block the service, select **Blocked** in the drop-down list.
   - To allow the service, select **Allowed** in the drop-down list.
4. Click the **Save** button.

Access to the selected service is blocked or allowed for the security policy or profile.

# Export of events to SIEM systems

This section describes how to configure export of events to the SIEM systems.

## Configuring event export to SIEM systems

Kaspersky Security Center Linux allows configuring event export to SIEM systems by one of the following methods: export to any SIEM system that uses Syslog format, export to Kaspersky SIEM, QRadar, Splunk, ArcSight SIEM systems that use LEEF and CEF formats, or export of events to SIEM systems directly from the Kaspersky Security Center database. When you complete this scenario, Administration Server sends events to a SIEM system automatically.

Prerequisites

Before you start configuration export of events in the Kaspersky Security Center Linux:

- Learn more about the methods of event export.
- Make sure that you have the values of system settings.

> You can perform the steps of this scenario in any order.

The process of export of events to a SIEM system consists of the following steps:

- **Configuring the SIEM system to receive events from Kaspersky Security Center Linux**

  How-to instructions: Configuring event export in a SIEM system

- **Selecting the events that you want to export to the SIEM system**

  Mark which events you want to export to the SIEM system. First, mark the general events that occur in all managed Kaspersky applications. Then, you can mark the events for specific managed Kaspersky applications.

- **Configuring export of events to the SIEM system**

  You can export events by using one of the following methods:

  - Using TCP, UDP, or TLS over TCP protocols.
  - Exporting events directly from the Kaspersky Security Center database. The Kaspersky Security Center database contains a collection of public views; you can find a description of these public views in the klakdb.chm document.

Results

After configuring export of events to a SIEM system you can view export results if you selected events which you want to export.

# Prerequisites

When setting up automatic export of events in the Kaspersky Security Center Linux, you must specify some of the SIEM system settings. It is recommended that you check these settings in advance in order to prepare for setting up Kaspersky Security Center Linux.

To successfully configure automatic sending of events to a SIEM system, you must know the following settings:

- **SIEM system server address**

  The IP address of the server on which the currently used SIEM system is installed. Check this value in your SIEM system settings.

- **SIEM system server port**

  Port number used to establish a connection between Kaspersky Security Center Linux and your SIEM system server. You specify this value in the Kaspersky Security Center Linux settings and in the receiver settings of your SIEM system.

- **Protocol**

  Protocol used for transferring messages from Kaspersky Security Center Linux to your SIEM system. You specify this value in the Kaspersky Security Center Linux settings and in the receiver settings of your SIEM system.

# About event export

Kaspersky Security Center Linux allows you to receive information about events that occur during the operation of Administration Server and Kaspersky applications installed on managed devices. Information about events is saved in the Administration Server database.

You can use event export within centralized systems that deal with security issues on an organizational and technical level, provide security monitoring services, and consolidate information from different solutions. These are SIEM systems, which provide real-time analysis of security alerts and events generated by network hardware and applications, or Security Operation Centers (SOCs).

These systems receive data from many sources, including networks, security, servers, databases, and applications. SIEM systems also provide functionality to consolidate monitored data in order to help you avoid missing critical events. In addition, the systems perform automated analysis of correlated events and alerts in order to notify the administrators of immediate security issues. Alerting can be implemented through a dashboard or can be sent through third-party channels such as email.

The process of exporting events from Kaspersky Security Center Linux to external SIEM systems involves two parties: an event sender, Kaspersky Security Center Linux, and an event receiver, a SIEM system. To successfully export events, you must configure this in your SIEM system and in the Kaspersky Security Center Linux. It does not matter which side you configure first. You can either configure the transmission of events in the Kaspersky Security Center Linux, and then configure the receipt of events by the SIEM system, or vice versa.

## Methods for sending events from Kaspersky Security Center Linux

There are three methods for sending events from Kaspersky Security Center Linux to external systems:

- Sending events over the Syslog protocol to any SIEM system

  Using the Syslog protocol, you can relay any events that occur on the Administration Server and in Kaspersky applications that are installed on managed devices. The Syslog protocol is a standard message-logging protocol. You can use it to export events to any SIEM system.

  For this purpose, you need to mark the events that you want to relay to the SIEM system. You can mark the events in Kaspersky Security Center Web Console. Only marked events will be relayed to the SIEM system. If you marked nothing, no events will be relayed.

- Sending events over the CEF and LEEF protocols to Kaspersky SIEM, QRadar, Splunk, and ArcSight systems

You can use the CEF and LEEF protocols to export general events. When exporting events over the CEF and LEEF protocols, you do not have the capability to select specific events to export. Instead, all general events are exported. To convert Kaspersky Security Center Linux events to events in the CEF and LEEF format, you need to use the siem_conversion_rules.xml file. This file contains the list of Kaspersky Security Center Linux event attributes and corresponding attributes of events in the CEF and LEEF format. Also, the siem_conversion_rules.xml file contains the rules for generating messages corresponding to events. This file is included in the Kaspersky Security Center Linux distribution kit.

Unlike the Syslog protocol, the CEF and LEEF protocols are not universal. CEF and LEEF are intended for the appropriate SIEM systems (Kaspersky SIEM, QRadar, Splunk, and ArcSight). Therefore, when you choose to export events over one of these protocols, you use the required parser in the SIEM system.

- Directly from the Kaspersky Security Center Linux database to any SIEM system

  This method of exporting events can be used to receive events directly from public views of the database by means of SQL queries. The results of a query are saved to an XML file that can be used as input data for an external system. Only events available in public views can be exported directly from the database.

### Receipt of events by the SIEM system

The SIEM system must receive and correctly parse the events received from Kaspersky Security Center Linux. To achieve this, you need to correctly configure the SIEM system. The configuration depends on the specific SIEM system utilized. However, there are a number of general steps in the configuration of all SIEM systems, such as configuring the receiver and the parser.

## About configuring event export in a SIEM system

The process of exporting events from Kaspersky Security Center Linux to external SIEM systems involves two parties: an event sender, Kaspersky Security Center Linux, and an event receiver, a SIEM system. You must configure the export of events in your SIEM system and in the Kaspersky Security Center Linux.

The settings that you specify in the SIEM system depend on the particular system that you are using. Generally, for all SIEM systems you must set up a receiver and, optionally, a message parser to parse received events.

### Setting up the receiver

To receive events sent by Kaspersky Security Center Linux, you must set up the receiver in your SIEM system. In general, the following settings must be specified in the SIEM system:

- **Export protocol**

  A message transfer protocol, either UDP, TCP, or TLS over TCP. This protocol must be the same as the protocol you specified in Kaspersky Security Center Linux.

- **Port**

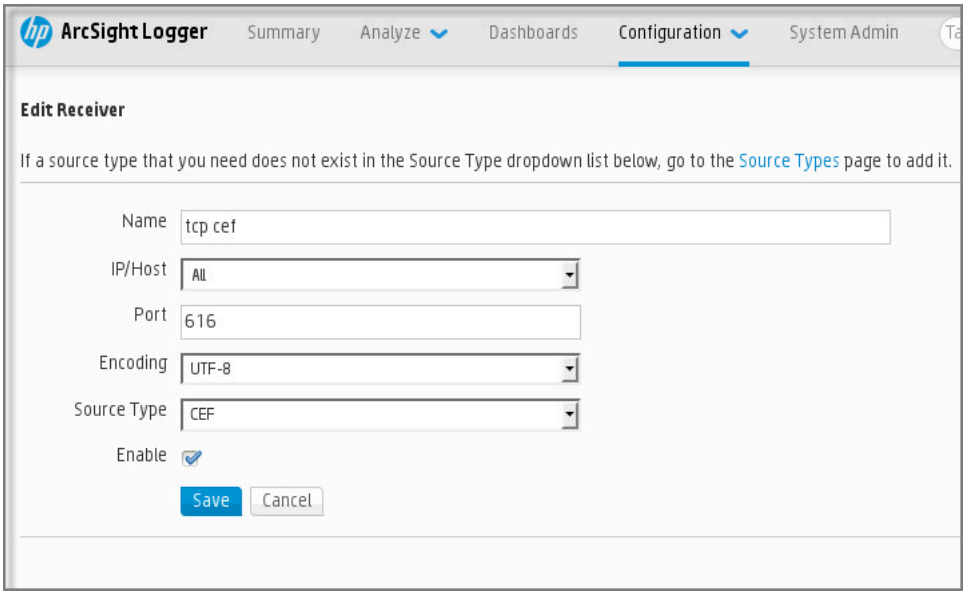
  Specify the port number to connect to Kaspersky Security Center Linux. This port must be the same as the port you specify in Kaspersky Security Center Linux during configuration with a SIEM system.

- **Data format**

  Specify the Syslog, CEF, or LEEF format.

Depending on the SIEM system that you use, you may have to specify some additional receiver settings.

The figure below shows the receiver setup screen in ArcSight.




Receiver setup in ArcSight

Message parser

Exported events are passed to SIEM systems as messages. A parser is then applied to these messages to make sure that the event information can be used by the SIEM system. A message parser is part of the SIEM system; it is used to split the contents of the message into fields such as event code, severity, description, parameters. This enables the SIEM system to process events received from Kaspersky Security Center Linux so that they can be stored in the SIEM system database.

# About exporting events using CEF and LEEF formats

You can use the CEF and LEEF formats to export to SIEM systems general events, policy change events, and the events transferred by Kaspersky applications to the Administration Server. The set of export events is predefined, and you cannot select the events to be exported. Before sending events to the SIEM system (Kaspersky SIEM, QRadar, ArcSight, or Splunk), it is necessary to interpret Kaspersky Security Center Linux events to events in the CEF and LEEF format by using the rules specified in the siem_conversion_rules.xml file.

Select the format of export on the basis of the SIEM system used. The table below shows SIEM systems and the corresponding formats of export.

Formats of event export to a SIEM system

| SIEM system | Format of export |
|---|---|
| Kaspersky SIEM | CEF |
| ArcSight | CEF |

| SIEM system | Format of export |
| --- | --- |
| Splunk | CEF |
| QRadar | LEEF |

- LEEF (Log Event Extended Format) is a specialized event format for the IBM Security QRadar SIEM. QRadar can receive, identify and process events transmitted over the LEEF protocol. LEEF events must use UTF-8 character encoding. You can find detailed information on LEEF protocol in IBM Knowledge Center.

- CEF (Common Event Format)—An open log management standard that improves the interoperability of security-related information from different security and network devices and applications. CEF enables you to use a common event log format so that data can easily be integrated and aggregated for analysis by an enterprise management system. CEF events must use UTF-8 character encoding.

Automatic export means that Kaspersky Security Center Linux sends general events to the SIEM system. Automatic export of events starts immediately after you enable it. This section explains in detail how to enable automatic event export.

# Converting events to the CEF or LEEF format

Before sending events to the SIEM system (Kaspersky SIEM, QRadar, ArcSight, or Splunk), it is necessary to interpret Kaspersky Security Center Linux events to events in the CEF and LEEF format by using the rules specified in the siem_conversion_rules.xml file. This file is included in the Kaspersky Security Center Linux distribution kit.

The siem_conversion_rules.xml file contains the predefined interpretation rules to convert events to the CEF and LEEF format. If you want to use additional event interpretation rules, you can add them to the file manually.

The siem_conversion_rules.xml file includes the following sections:

- `<product name="SP_QRADAR" vendor="IBM">`

  This section contains rules for generating events in the LEEF format, which can be exported to the QRadar SIEM system.

- `<product name="SP_ARCSIGHT" vendor="HP">`.

  This section contains rules for generating events in the CEF format, which can be exported to the ArcSight or Splunk SIEM system.

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`.

  This section contains rules for generating events in the CEF format, which can be exported to KUMA.

Each section has the `<common>` subsection, in which Kaspersky Security Center Linux event attributes and corresponding attributes of events in the LEEF format are located. These common attributes are used for all types of events that can be exported.

Also, each section has the `<event>` subsections. Each `<event>` subsection contains additional attributes that are added to those listed in the `<common>` section.

You can add a new event generation rule to the siem_conversion_rules.xml file manually.

*To add a new event generation rule:*

1. Add a new `<event>` subsection to the `<product name="SP_QRADAR" vendor="IBM">`, `<product name="SP_QRADAR" vendor="IBM">`, or `<product name="Kaspersky SIEM" vendor="Kaspersky">` section, and then specify the additional event attributes, if needed.

2. If an event consist only of common attributes, the `<event>` subsection will be empty.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center Linux 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 Linux 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>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Kaspersky Security Center Linux 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>
```

# Marking of events for export to SIEM systems in Syslog format

After enabling automatic export of events, you must select which events will be exported to the external SIEM system.

You can configure export of events in the Syslog format to an external system based on one of the following conditions:

- Marking general events. If you mark events to export in a policy, in the settings of an event, or in the Administration Server settings, the SIEM system will receive the marked events that occurred in all applications managed by the specific policy. If exported events were selected in the policy, you will not be able to redefine them for an individual application managed by this policy.

- Marking events for a managed application. If you mark events to export for a managed application installed on a managed device, the SIEM system will receive only the events that occurred in this application.

For policy change events, you can only enable or disable the export of all such events to a SIEM system.

## Marking events of a Kaspersky application for export in the Syslog format

If you want to export events that occurred in a specific managed application installed on the managed devices, mark the events for export in the application policy. In this case, the marked events are exported from all of the devices included in the policy scope.

*To mark events for export for a specific managed application:*

1. In the main menu, go to **Asset management** → **Policies**.
2. Click the policy of the application for which you want to mark events.

   The policy settings window opens.
3. Go to the **Event configuration** section.
4. Select the check boxes next to the events that you want to export to a SIEM system.
5. Click the **Mark for export to SIEM system by using Syslog** button.

   > You can also mark an event for export to a SIEM system in the **Event registration** section, which opens by clicking the link of the event.

6. A check mark (✓) appears in the **Syslog** column of the event or events that you marked for export to the SIEM system.
7. Click the **Save** button.

The marked events from the managed application are ready to be exported to a SIEM system.

You can mark which events to export to a SIEM system for a specific managed device. If previously exported events were marked in an application policy, you will not be able to redefine the marked events for a managed device.

*To mark events for export for a managed device:*

1. In the main menu, go to **Asset management** → **Managed devices**.

   The list of managed devices is displayed.

2. Click the link with the name of the required device in the list of managed devices.

   The properties window of the selected device is displayed.

3. Go to the **Applications** section.

4. Click the link with the name of the required application in the list of applications.

5. Go to the **Event configuration** section.

6. Select the check boxes next to the events that you want to export to a SIEM system.

7. Click the **Mark for export to SIEM system by using Syslog** button.

   > You can also mark an event for export to a SIEM system in the **Event registration** section, which opens by clicking the link of the event.

8. A check mark (✓) appears in the **Syslog** column of the event or events that you marked for export to the SIEM system.

From now on, Administration Server sends the marked events to the SIEM system if export to the SIEM system is configured.

## Marking general events for export in Syslog format

You can mark general events that Administration Server will export to SIEM systems by using the Syslog format.

*To mark general events for export to a SIEM system:*

1. In the main menu, do one of the following:

   - Click the Administration Server name.
   - Go to **Asset management** → **Policies**, and then click a link of a policy.

2. In the window that opens, go to the **Event configuration** tab.

3. Click **Mark for export to SIEM system by using Syslog**.

   > You can also mark an event for export to a SIEM system in the **Event registration** section, which opens by clicking the link of the event.

4. A check mark (✓) appears in the **Syslog** column of the event or events that you marked for export to the SIEM system.

From now on, Administration Server sends the marked events to the SIEM system if export to the SIEM system is configured.

# About exporting events using Syslog format

You can use the Syslog format to export to SIEM systems the events that occur in Administration Server and other Kaspersky applications installed on managed devices.

Syslog is a standard for message logging protocol. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type that generates the message, and is assigned a severity level.

The Syslog format is defined by Request for Comments (RFC) documents published by the Internet Engineering Task Force (internet standards). The RFC 5424 standard is used to export the events from Kaspersky Security Center Linux to external systems.

In Kaspersky Security Center Linux, you can configure export of the events to the external systems using the Syslog format.

The export process consists of two steps:

1. Enabling automatic event export. At this step, Kaspersky Security Center Linux is configured so that it sends events to the SIEM system. Kaspersky Security Center Linux starts sending events immediately after you enable automatic export.

2. Selecting the events to be exported to the external system. At this step, you select which event to export to the SIEM system.

# Configuring Kaspersky Security Center Linux for export of events to a SIEM system

To export events to a SIEM system, you have to configure the process of export in Kaspersky Security Center Linux.

Before sending events to the SIEM system (Kaspersky SIEM, QRadar, ArcSight, or Splunk), it is necessary to interpret Kaspersky Security Center Linux events to events in the CEF and LEEF format by using the rules specified in the siem_conversion_rules.xml file.

*To configure export to SIEM systems in the Kaspersky Security Center Web Console:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Export to SIEM** section.

3. Click the **Configure connection** link.

   The **Export settings** section opens.

4. Specify the settings in the **Export settings** section:

- **SIEM system server address**

  The IP address of the server on which the currently used SIEM system is installed. Check this value in your SIEM system settings.

- **SIEM system port**

  Port number used to establish a connection between Kaspersky Security Center Linux and your SIEM system server. You specify this value in the Kaspersky Security Center Linux settings and in the receiver settings of your SIEM system.

- **Protocol**

  Select the protocol to be used for transferring messages to the SIEM system. You can select TCP, UDP, or TLS over TCP protocol.

  Specify the following TLS settings if you select the TLS over TCP protocol:

  - **Server authentication**

    In the **Server authentication** field, you can select the **Trusted certificates** or **SHA fingerprints** values:

    - **Trusted certificates**. You can receive a complete certificate chain (including the root certificate) from a trusted certification authority (CA) and upload the file to Kaspersky Security Center Linux. Kaspersky Security Center Linux checks whether the certificate chain of the SIEM system server is also signed by a trusted CA or not.

      To add a trusted certificate, click the **Browse for CA certificates file** button, and then upload the certificate.

    - **SHA fingerprints**. You can specify SHA1 thumbprints of the complete certificate chain of the SIEM system (including the root certificate) in Kaspersky Security Center Linux. To add a SHA1 thumbprint, enter it in the **Thumbprints** field, and then click the **Add** button.

    By using the **Add client authentication** setting, you can generate a certificate to authenticate Kaspersky Security Center Linux. Thus, you will use a self-signed certificate issued by Kaspersky Security Center Linux. In this case, you can use both a trusted certificate and a SHA fingerprint to authenticate the SIEM system server.

  - **Add Subject name/Subject alternative name**

    Subject name is a domain name for which the certificate is received. Kaspersky Security Center Linux cannot connect to the SIEM system server if the domain name of the SIEM system server does not match the subject name of the SIEM system server certificate. However, the SIEM system server can change its domain name if the name has changed in the certificate. In this case, you can specify subject names in the **Add Subject name/Subject alternative name** field. If any of the specified subject names matches the subject name of the SIEM system certificate, Kaspersky Security Center Linux validates the SIEM system server certificate.

  - **Add client authentication**

For client authentication, you can insert your certificate or generate it in Kaspersky Security Center Linux.

- **Insert certificate**. You can use a certificate that you received from any source, for example, from any trusted CA. You must specify the certificate and its private key by using one of the following certificate types:

  - **X.509 certificate PEM**. Upload a file with a certificate in the **File with certificate** field, and a file with a private key in the **File with key** field. Both files do not depend on each other and the order of loading of the files is not significant. When both files are uploaded, specify the password for decoding the private key in the **Password or certificate verification** field. The password can have an empty value if the private key is not encoded.

  - **X.509 certificate PKCS12**. Upload a single file that contains a certificate and its private key in the **File with certificate** field. When the file is uploaded, specify the password for decoding the private key in the **Password or certificate verification** field. The password can have an empty value if the private key is not encoded.

- **Generate key**. You can generate a self-signed certificate in Kaspersky Security Center Linux. As a result, Kaspersky Security Center Linux stores the generated self-signed certificate, and you can pass the public part of the certificate or SHA1-fingerprint to the SIEM system.

- **Data format**

  You can select Kaspersky SIEM, IBM QRadar SIEM, ArcSight, Splunk, or System log formats, depending on the requirements of the SIEM system.

  If you select the System log data format, you must specify **Maximum message size, in bytes**.

  Specify the maximum size (in bytes) of one message relayed to the SIEM system. Each event is relayed in one message. If the actual length of a message exceeds the specified value, the message is truncated and data may be lost. The default size is 2048 bytes. This field is available only if you selected the System log format in the **Protocol** field.

5. If you want, you can export archived events from the Administration Server database and set the start date from which you want to start the export of archived events:

   a. Click the **Set the export start date** link.

   b. In the section that opens, specify the start date in the **Date to start export from** field.

   c. Click **OK**.

6. Enable the **Export events to SIEM** option.

7. To send policy change events to SIEM, enable the **Export extended events for policy changes to SIEM** option. A separate event will be sent to SIEM for each changed policy setting.

8. To check that the SIEM system connection is configured, click the **Check connection** button.

   The connection with the SIEM system server is established, and a test event is sent. The connection status will be displayed.

9. Click the **Save** button.

Export to a SIEM system is configured. From now on, if you configured the receiving of events in a SIEM system, Administration Server exports the marked events or policy change events to a SIEM system. If you set the start date of export, Administration Server also exports the marked events stored in the Administration Server database from the specified date.

# Monitoring of policy and policy profile changes

When a policy setting is changed, a policy change event is generated, which you can then export to a SIEM system to monitor policy changes and generate alerts. Policy change events can only be accessed through a SIEM system.

Policy change events are not stored in the Administration Server database after generation and cannot be viewed in the **Monitoring** → **Event selections** section of Kaspersky Security Center Web Console. You also cannot specify notification settings and storage settings for these events on the **Event configuration** tab.

When you create a policy, the policy change event is generated for each policy setting. When you change a policy, the policy change event is generated for every changed setting of a policy. Deletion of a policy generates one event. For example, Kaspersky Security Center policy creation generates around 1000 events, and Kaspersky Endpoint Security policy creation generates more than 7000 events.

## Conditions for generating policy change events

A policy change event is generated whenever a user performs any of the following actions with a policy or policy profile:

- Create, edit, or delete a policy
- Create, edit, or delete a policy profile
- Roll back the policy to a selected revision
- Import or copy a policy
- Import or copy a policy profile
- Move a policy to another administration group

A policy modification event is generated when the following conditions are satisfied:

- The policies of the following applications are changed:
  - Kaspersky Security Center Network Agent
  - Kaspersky Security Center Administration Server
  - Kaspersky Endpoint Security for Windows 14.1 or later
  - Kaspersky Endpoint Security for Linux 12.5 or later
  - Kaspersky Endpoint Security for Linux 12.4 or later
  - Kaspersky Endpoint Security for Mac 12.2.1 or later

- The **Export extended events for policy changes to SIEM** option in the Administration Server properties is enabled.
- Policy is modified manually through Kaspersky Security Center Web Console interface.

Policy change events are not created in the following cases:

- General policy settings are modified.
- Policy settings inherited from a parent policy are modified.
- Policy settings are changed via the Kaspersky Security Center OpenAPI.
- Kaspersky application settings are modified directly in the application.

### Policy change event fields

The table below shows a set of policy change event field. The representation of these fields depends on the output event format (for example, Syslog, CEF, or LEEF). For the exact field names and event templates, refer to the siem_conversion_rules.xml file. Event parameters are available only in English.

| Event field | Data type | Description |
|---|---|---|
| `eventType` | string | Type of the event. Allows creating correlation rules for the specific type of event.<br>Possible values: "Policy created", "Policy modified", "Policy deleted". |
| `srvName` | string | Administration Server name. |
| `eventTime` | datetime | Date and time of the event (in UTC). |
| `eventGroupID` | int | ID of the event group of a modification. |
| `objectID` | int | Internal ID of an object. |
| `objectName` | string | Policy display name. |
| `objectGroup` | string | Full path and name of the administration group that contains the policy. |
| `user` | string | Name of the user that authored the modification. |
| `operation` | string | Parameter modification's type.<br>Possible values: "Added", "Removed", "Changed". |
| `path` | string | Parameter's path. Contains the path to the parent node of the end parameter. The path is created based on the names of the policy's sections and subsections. The path structure is identical to the ones described in Network Agent policy settings, General policy settings, and Comparing policy revisions. |
| `parameter` | string | The name of the modified policy setting. |
| `oldValue` | string | Old value of the end parameter. |
| `newValue` | string | New value of the end parameter. |

# Exporting events directly from the database

You can retrieve events directly from the Kaspersky Security Center Linux database without having to use the Kaspersky Security Center Linux interface. You can either query the public views directly and retrieve the event data, or create your own views on the basis of existing public views and address them to get the data you need.

Public views

For your convenience, a set of public views is provided in the Kaspersky Security Center Linux database. You can find the description of these public views in the klakdb.chm document.

The v_akpub_ev_event public view contains a set of fields that represent the event parameters in the database. In the klakdb.chm document you can also find information on public views corresponding to other Kaspersky Security Center Linux entities, for example, devices, applications, or users. You can use this information in your queries.

This section contains instructions for executing an SQL query by means of the klsql2 utility and a query example.

To create SQL queries or database views, you can also use any other program for working with databases. Information on how to view the parameters for connecting to the Kaspersky Security Center Linux database, such as instance name and database name, is given in the corresponding section.

## Executing an SQL query by using the klsql2 utility

This article describes how to use the klsql2 utility, and execute an SQL query by using this utility. Use klsql2 utility version that is included in your Kaspersky Security Center Linux version installed.

*To use the klsql2 utility:*

1. Go to the directory where Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.
2. In this directory, create a blank file with the .sql extension.
3. Open the created .sql file in any text editor.
4. In the .sql file, type the SQL query that you want, and then save the file.
5. On the device with Administration Server installed, in the command line, type the following command to execute the SQL query from the .sql file and save the results to the result.xml file:
   ```
   sudo ./klsql2 -i src.sql -u <username> -p <password> -o result.xml
   ```
   where <username> and <password> are credentials of the user account that has access to the database.
6. If required, enter the login and password of the user account that has access to the database.
7. Open the newly created result.xml files to view the SQL query results.

You can edit the .sql file and create any SQL query to the public views. Then, from the command line, execute your query and save the results to a file.

## Example of an SQL query in the klsql2 utility

This section shows an example of an SQL query, executed by means of the klsql2 utility.

The following examples illustrate retrieval of the events that occurred on devices during the last seven days, and display of the events ordered by the time they occur. The most recent events are displayed first.

Example for PostgreSQL:

```
SELECT
  /* event identifier */
  "e"."nId",

  /* time, when the event occurred */
  "e"."tmRiseTime",

  /* internal name of the event type */
  "e"."strEventType",

  /* displayed name of the event */
  "e"."wstrEventTypeDisplayName",

  /* displayed description of the event */
  "e"."wstrDescription",

  /* displayed description of the event */
  "e"."wstrGroupName",

  /* displayed name of the device, on which the event occurred */
  "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))  || '.'  ||

    /* IP address of the device, on which the event occurred */
    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 ;
```

Example for MySQL or MariaDB:

```
SELECT

  /* event identifier */
  `e`.`nId`,

  /* time, when the event occurred */
  `e`.`tmRiseTime`,

  /* internal name of the event type */
  `e`.`strEventType`,

  /* displayed name of the event */
  `e`.`wstrEventTypeDisplayName`,

  /* displayed description of the event */
  `e`.`wstrDescription`,

  /* device group name */
  `e`.`wstrGroupName`,

  /* displayed name of the device, on which the event occurred */
  `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), '.',

    /* IP address of the device, on which the event occurred */
    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 ;
```

## Viewing the Kaspersky Security Center Linux database name

If you want to access Kaspersky Security Center Linux database by means of the MySQL, or MariaDB database management tools, you must know the name of the database in order to connect to it from your SQL script editor.

*To view the name of the Kaspersky Security Center Linux database:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Details of current database** section.

   The database name is specified in the **Database name** field. Use the database name to address the database in your SQL queries.

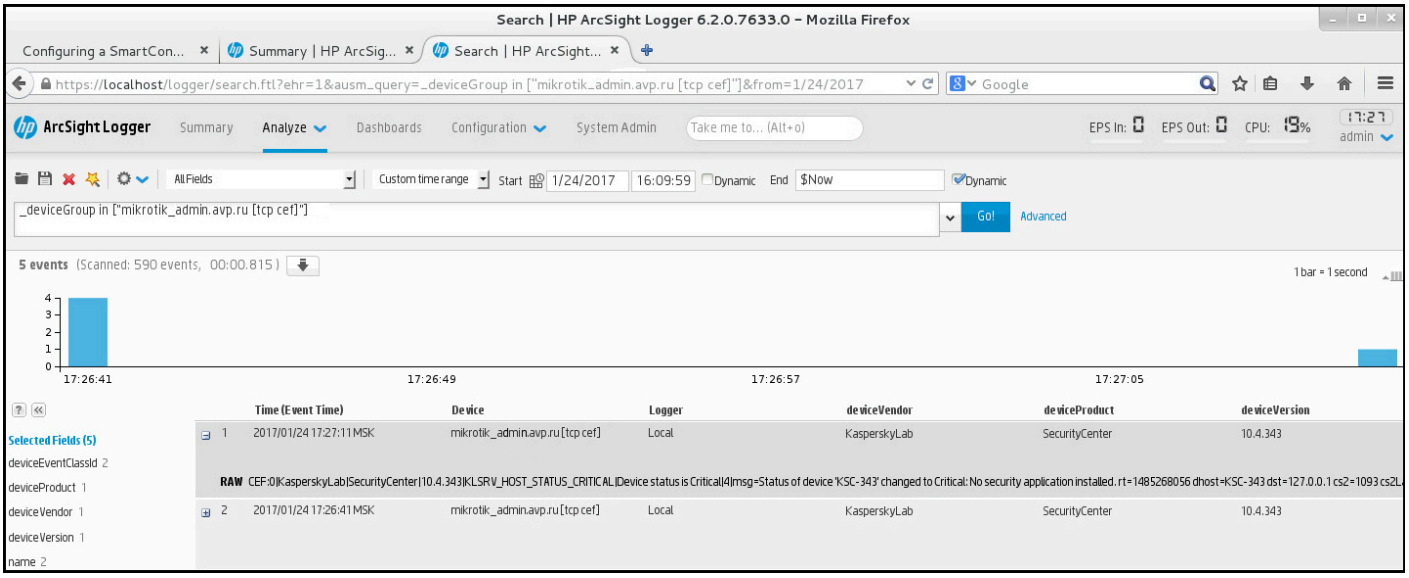
# Viewing export results

You can control for successful completion of the event export procedure. To do this, check whether messages with export events are received by your SIEM system.

If the events sent from Kaspersky Security Center Linux are received and properly parsed by your SIEM system, configuration on both sides is done properly. Otherwise, check the settings you specified in Kaspersky Security Center Linux against the configuration in your SIEM system.

The figure below shows the events exported to ArcSight. For example, the first event is a critical Administration Server event: "*Device status is Critical*".

The representation of export events in the SIEM system varies according to the SIEM system you use.




Example of events

# Managing object revisions

This section contains information about object revision management.

The *revision* is the state of an object at a certain moment. Each time you create or modify an object, a new revision of that object is created. Each revision contains all object settings as they are at the time when the revision is created or saved.

Objects that support revision management include:

- Administration Server properties
- Policies
- Tasks
- Administration groups
- User accounts
- Installation packages

You can perform the following actions on object revisions:

- View a selected revision (available only for policies)
- Roll back changes made to an object to a selected revision
- Save revisions as a JSON file (available only for policies)

In the properties window of any object that supports revision management, the **Revision history** section displays a list of object revisions with the following details:

- **Revision**—Object revision number.
- **Time**—Date and time the object was modified.
- **User**—Name of the user who modified the object.
- **User device IP address**—IP address of the device from which the object was modified.
- **Web Console IP address**—IP address of Kaspersky Security Center Web Console with which the object was modified.
- **Action**—Action performed on the object.
- **Description**—Description of the revision related to the change made to the object settings.

  By default, the object revision description is blank. To add a description to a revision, select the relevant revision and click the **Edit description** button. In the opened window, enter some text for the revision description.

# Viewing and saving a policy revision

A policy revision is a saved state of a policy that is automatically created every time it is changed or saved. A revision contains policy settings, profiles, and rules for their activation, metadata about the date and the user and IP address that the revision was created by. Kaspersky Security Center Linux lets you view policy revisions to track changes of settings; you can also save a revision to a JSON file.

Viewing and saving a policy revision are available if the corresponding management web plug-in supports this functionality.
The options are available for the policies of Administration Server, Network Agent, Kaspersky Endpoint Security for Windows (starting from version 14.0 of the web plug-in), Kaspersky Endpoint Security for Linux (starting from version 12.4 of the web plug-in) and Kaspersky Endpoint Security for Mac (starting from 12.2.1 Patch A version of the web plug-in).

*To view a policy revision:*

1. In the main menu, go to **Asset management** → **Policies**.
2. Click the policy for the revision that you want to view, and then go to the **Revision history** section.
3. In the list of policy revisions, click the number of the revision that you want to view.

   The displayed report provides information about the settings of the policy, its profiles, and the activation rules for them.

   If the revision size is more than 10 MB, you will not be able to view it by using Kaspersky Security Center Web Console. You will be prompted to save the selected revision to a JSON file.

   If the revision size does not exceed 10 MB, a report in the HTML format with the settings of the selected policy revision is displayed. Since the report is displayed in a pop-up window, ensure that pop-ups are allowed in your browser.

For the policies of Kaspersky Endpoint Security for Windows and Kaspersky Endpoint Security for Mac, the report will not contain information about the policy profiles.

*To save a policy revision to a JSON file,*

In the list of policy revisions, select the revision that you want to save, and then click **Save to file**.

The revision is saved to a JSON file.

If necessary, you can compare policy revisions.

# Comparing policy revisions

You can compare past revisions of a policy to its current revision, compare different revisions selected in the list, or compare a revision of one policy to a revision of another policy. The options are available for the policies of Administration Server, Network Agent, Kaspersky Endpoint Security for Windows (starting from 14.0 web plug-in version), and Kaspersky Endpoint Security for Mac (starting from 12.2.1 Patch A web plug-in version).

Comparison of policy revisions is available if the relevant management web plug-ins support this functionality.

*To compare revisions of a policy:*

1. In the main menu, go to **Asset management** → **Policies**.
2. Click the policy whose revisions you want to compare.

   The policy settings window opens.
3. Go to the **Revision history** tab, and then select the check boxes next to the revisions to be compared.
4. In the toolbar, click the **Compare** button, and then from the drop-down list, select one of the following options:

   - **With current revision**, if you want to compare the revision that you selected at step 3 with the last saved revision of the same policy.
   - **Selected revisions**, if you want to compare the two revisions whose check boxes you selected at step 3.

     The order of selecting check boxes does not affect the comparison results. By default, the earlier revision of the selected revision is compared to the latest revision. For example, if you select check boxes next to the revisions 5 and 1, revision 1 is compared to revision 5. The report will contain information about the settings in revision 1 that were added, removed, or changed compared to the revision 5.
   - **With another policy revision**, if you want to compare the revisions of two different policies.

     In the right pane that opens, do the following:

     a. In the **Application name** field, select the policy you want to compare: Network Agent or Administration Server.

     b. In the **Policy name** field, specify the name of the policy whose revision you want to compare with the one you selected at step 3.

     The list of the policy revisions is displayed.

     c. Select the required revision, and then click the **Compare** button.

A report on the revisions comparison is displayed in HTML format on a new tab of your browser.

If the comparison result exceeds 10 MB, the corresponding dialog box is displayed. You can either click the **Save to file** button to save the report as a file, or cancel the operation.

The report is displayed in the interface language of your Kaspersky Security Center Web Console. You can expand some sections of the report by clicking the arrow down icon (▾) next to the section or collapse the section by clicking the arrow up (▴) icon.

The report contains the following information:

- Kaspersky logo.
- The report name.
- Time and date of the report creation.
- The policy name, Administration Server, and administration group that includes the policy (policies) whose revisions were compared.
- The **Save as HTML** button. If you click the button, the report will be saved to your computer.
- The **Summary** section that displays general information on the compared revisions: policy (policies) name, revision number, time and date when the revision was saved, the user who saved the revision, and the revision description.

  For inherited polices, the user is not displayed.

- Differences between the compared revisions. The differences are displayed in the following sections:
  - **Added settings**
  - **Removed settings**
  - **Changed settings**
  - **Settings only available for object 1** (if you compared the revisions of two different policies)
  - **Settings only available for object 2** (if you compared the revisions of two different policies)

  A section is not displayed if it has no data.

# Rolling back an object to a previous revision

You can roll back changes made to an object, if necessary. For example, you may have to revert the settings of a policy to their state on a specific date.

*To roll back changes made to an object:*

1. In the object's properties window, open the **Revision history** tab.
2. In the list of object revisions, select the revision that you want to roll back changes for.

3. Click the **Roll back** button.

4. Click **OK** to confirm the operation.

The object is now rolled back to the selected revision. The list of object revisions displays a record of the action that was taken. The revision description displays information about the number of the revision to which you reverted the object.

Rolling back operation is available only for policy and task objects.

# Active threats

Information about unprocessed files that have been detected on client devices is stored in the **Repositories** section, **Active threats** subsection.

Postponed processing and disinfection are performed by the security application upon request or after a specified event occurs. You can configure the postponed processing.

## Disinfecting an unprocessed file

*To start disinfection of an unprocessed file:*

1. In the main menu, go to **Repositories** → **Active threats**.

2. Do one of the following:

   - Select the check box next to the file that you have to disinfect.

   - Click the name of the file that you have to disinfect.

3. Start disinfection of the file by clicking the **Disinfect** button.

The attempt to disinfect the selected file is then performed.

If the file is disinfected, the security application installed on the client device restores it to its original folder. The record of the file is removed from the list in the **Active threats** section. If the file cannot be disinfected, the security application installed on the device deletes it from that device. The record of the file is removed from the list in the **Active threats** section.

File disinfection and deletion capability may vary depending on which security application is installed, its version, and settings.

# Downloading an unprocessed file

Kaspersky Security Center Linux allows you to download copies of unprocessed files found on client devices. This refers to files treated or deleted by the application. The files are downloaded to the device with Kaspersky Security Center Linux installed, to the specified folder.

You can download copies of files if the files were deleted or modified during disinfection and their copies are stored in the Kaspersky Endpoint Security for Linux storage on the managed device.

*To download a copy of an unprocessed file:*

1. In the main menu, go to **Repositories** → **Active threats**.
2. Do one of the following:
   - Select the check box next to the file that you have to download.
   - Click the name of the file that you have to download.
3. Start downloading by clicking the **Download** button.

The security application installed on the client device on which the unprocessed file has been found downloads a copy of that file to the specified folder.

# Deleting files from the Active threats section

*To delete a file from the **Active threats** section:*

1. In the main menu, go to **Repositories** → **Active threats**.
2. Do one of the following:
   - Select the check box next to the file that you have to delete.
   - Click the name of the file that you have to delete.
3. Delete the files by clicking the **Delete** button.
4. In the window that opens, click the **Delete** button.

   The security applications that placed the files in repositories on client devices will delete the same files from those repositories. The records of the files are removed from the list in the **Active threats** section.

# Deletion of objects

This section provides information about deleting objects.

You can delete objects, including the following:

- Policies
- Tasks
- Installation packages
- Virtual Administration Servers
- Users
- Security groups
- Administration groups

*To delete an object:*

1. Open the required section of the Kaspersky Security Center Web Console, and then select the object.
2. In the toolbar, click the **Delete** button.
3. In the window that opens, click **OK** to confirm your selection.

   The selected object is deleted.

When you delete an object, information about it remains in the database. The storage term for information about the deleted objects is the same as the storage term for object revisions (the recommended term is 90 days). You can change the storage term only if you have the **Modify** permission in the **Deleted objects** area of rights.

## About deletion of client devices

When you delete a managed device from an administration group, the application moves the device to the Unassigned devices group. After device deletion, the installed Kaspersky applications—Network Agent and any security application, for example Kaspersky Endpoint Security—remain on the device.

Kaspersky Security Center Linux handles the devices in the Unassigned devices group according to the following rules:

- If you have configured device moving rules and a device meets the criteria of a moving rule, the device is automatically moved to an administration group according to the rule.
- The device is stored in the Unassigned devices group and automatically removed from the group according to the device retention rules.

  The device retention rules do not affect the devices that have one or more drives encrypted with full disk encryption. Such devices are not deleted automatically—you can only delete them manually. If you need to delete a device with an encrypted drive, first decrypt the drive, and then delete the device.

When you delete a device with encrypted drive, the data required to decrypt the drive is also deleted. If you select the **I understand the risk and want to delete the selected device(s)** check box in the confirmation window that opens when you delete such devices (either from the **Unassigned devices** or the **Managed Devices** group), it means that you are aware of the subsequent data deletion.

To decrypt the drive, the following conditions must be met:

- The device is reconnected to Administration Server to restore the data required to decrypt the drive.
- The device user remembers the decryption password.
- The security application that was used to encrypt the drive, for example Kaspersky Endpoint Security for Windows, is still installed on the device.

If the drive was encrypted by Kaspersky Disk Encryption technology, you can also try recovering data by using the FDERT Restore Utility.

In VDI, if you have a device with encrypted drives, the information on the encrypted drive is deleted after you delete the device.

When you delete a device from the Unassigned devices group manually, the application removes the device from the list. After device deletion, the installed Kaspersky applications (if any) remain on the device. Then, if the device is still visible to Administration Server and you have configured regular network polling, Kaspersky Security Center Linux discovers the device during the network polling and adds it back to the Unassigned devices group. Therefore, it is reasonable to delete a device manually only if the device is invisible to Administration Server.

# Downloading and deleting files from Quarantine and File backups

This section gives information on how to download and how to delete files from Quarantine and File backups in Kaspersky Security Center Web Console.

## Downloading files from Quarantine and File backups

You can download files from Quarantine and File backups only if one of the two conditions is met: either the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, or a connection gateway is in use. Otherwise, the downloading is not possible.

*To save a copy of file from Quarantine or File backups to a hard drive:*

1. Do one of the following:

   - If you want to save a copy of file from Quarantine, in the main menu, go to **Operations** → **Repositories** → **Quarantine**.

   - If you want to save a copy of file from Backup, in the main menu, go to **Operations** → **Repositories** → **File backups**.

2. In the window that opens, select a file that you want to download and click **Download**.

   The download starts. A copy of the file that had been placed in Quarantine on the client device is saved to the specified folder.

# About removing objects from the Quarantine, File backups, or Active threats repositories

When Kaspersky security applications installed on client devices place objects to the Quarantine, Backup, or Active threats repositories, they send the information about the added objects to the **Quarantine**, **File backups**, or **Active threats** sections in Kaspersky Security Center Linux. When you open one of these sections, you can remove the required object.

For the **File backups** or **Active threats** section, select an object from the list and click the **Remove** button.

For the **Quarantine** section, you can do one of the following:

- Select the check box next to the name of an object to be removed, and then in the toolbar, click the **Delete** button.

- Click the name of the object to be removed, and in the details window that opens, in the toolbar, click the **Delete** button.

  In this case, the object is deleted, a corresponding notification is displayed on the screen, and the details window is closed.

Kaspersky Security Center Linux either removes the selected object from the list, or deletes the selected object from the repository. The action to perform is defined by the Kaspersky application that placed the selected object to the repository. The Kaspersky application is specified in the **Entry added by** field.

For details about which action is to be performed, refer to the documentation of the Kaspersky application.

# Managing the application over SNMP

This section describes how to obtain information from Administration Server by using SNMP (Simple Network Management Protocol) in Linux.

SNMP is a protocol for managing network devices.

To work over SNMP, Kaspersky Security Center Linux uses the snmpd service included in the operating system and an SNMP agent to monitor Administration Server performance and send data to side applications by using OIDs. Kaspersky Security Center Linux can send this information in the form of statistics or SNMP traps, which are notifications about application events.

The SNMP allows you to access the following information about the application:

- General information
- Kaspersky Security Center Linux statistics since the installation of the application
- Information about Kaspersky Security Center Linux events

Read-only access is granted.

Information about SNMP traps and statistics sent over SNMP is stored in the adminkit.mib file. By default, the adminkit.mib file is located in the /opt/kaspersky/ksc64/share/snmp/ folder.

The local snmpd service on each cluster node serves as the SNMP server receiving the statistics. Interaction with an external SNMP server is not supported. SNMP traps can be received by using the snmptrapd service locally on each cluster node, or they can be redirected to an external server.

For operations over SNMP, preconfigure the snmpd service in the operating system on each cluster node.

# Configuring the snmpd service in the operating system

Before configuring, make sure that the snmpd service is installed in your operating system.

Creating a user account for access to the data

Before creating the account, stop the snmpd service by running the following command:

```
bash
sudo systemctl stop snmpd
```

To ensure the security of access to the data over SNMPv3 with authentication and encryption, you need to create a user account on the snmpd service side with the following information:

- User name (case-sensitive)
- Authentication algorithm (MD5 or SHA — SHA is recommended)
- Authentication password
- Encryption algorithm (only AES supported)
- Encryption password

You can create a user account in the following ways:

- By using the net-snmp-create-v3-user utility, if available in the operating system.
- Manually, by adding the appropriate directive to the configuration file of the snmpd service.

*To create a user account by using the net-snmp-create-v3-user utility, run the following command:*

```
net-snmp-create-v3-user -ro -a <authentication algorithm> -x <encryption algorithm> <user name>
```

Authentication and encryption passwords are requested interactively.

For example:

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

*To create a user account manually:*

1. Create the /var/lib/snmp/snmpd.conf configuration file by running the following command:

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

2. Add the following lines to the configuration file:

   ```
   createUser <user name> <authentication algorithm> "<authentication password>" <encryption algorithm> "
   <encryption password>"
   ```

   For example:

   ```
   createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"
   ```

### Creating a user account for receiving SNMP traps

To receive SNMP traps over SNMPv3 with authentication and encryption, you need to create an account on the side of the monitoring system in the context of the corresponding service (usually the snmptrapd service).

The account must contain the following information:

- User name
- Authentication algorithm
- Authentication password

- Encryption algorithm
- Encryption password

> For security purposes, use separate user accounts for access to data and for receiving SNMP traps.

For instructions on creating a user account for receiving SNMP traps, refer to the documentation of your monitoring system.

### Configuring the snmpd service

The configuration of the snmpd service is stored in the /etc/snmp/snmpd.conf file. You can add the necessary information to an existing configuration file, or create a new configuration file and add the lines listed below, in the order given.

> If you chose to create a new configuration file, make sure that only the superuser has access to it. If the required access permissions are not set, configure them by running the following commands in the specified order:
> `chown root:root /etc/snmp/snmpd.conf`
> `chmod 600 /etc/snmp/snmpd.conf`

*To configure the snmpd service:*

1. In the configuration file, specify the protocol, network interface address, and port number on which the snmpd service must listen for incoming requests.
   - If you want to listen for requests on all network interfaces, add the following lines to the configuration file:

     ```
     agentAddress udp:161
     ```

   - If you want to listen for requests only on the local network interface, for example, if the monitoring system is installed on the same machine, add the following lines to the configuration file:

     ```
     agentAddress udp:127.0.0.1:161
     ```

2. Configure interaction between Kaspersky Security Center Linux and the snmpd service. You can use either a UNIX socket or a TCP socket.
   - If you use a UNIX socket:
     a. Specify the path and permissions for the UNIX socket. To do this, add the following lines to the configuration file:

        ```
        master agentx
        agentXSocket unix:/var/run/agentx-master.socket
        agentXPerms 770 770 kluser klusers
        ```

     b. Add the klusers group as a supplementary group for the {'KLSRV_UNATT_KLSVCUSER'} account.

- If you use a TCP socket, specify the port and the address for the TCP socket. To do this, add the following lines to the configuration file:

```
master agentx
agentXSocket tcp:127.0.0.1:705,tcp6:[::1]:705
```

3. Set the minimum response timeout to at least 30 seconds. To do this, add the following lines to the configuration file:

```
agentxTimeout 30
```

4. If necessary, you can provide a description of the server where SNMP is configured, location of the system, and the contact address of the administrator. To do this, add the following lines to the configuration file:

```
sysDescr <server description>
sysLocation <server location>
sysContact <contact address of the administrator>
sysServices 72
```

5. Specify the scope of the OID tree that you want to be available to your monitoring system via the SNMP protocol. To do this, add the following lines to the configuration file:

```
view monitoring included .1.3.6.1.4.1.23668.1093.1

view systemonly included .1.3.6.1.4.1.23668.1093.1
```

6. If necessary, you can additionally specify the scope of the OID tree containing information about the operating system that is stored by the snmpd service. This scope will be available to your monitoring system.

   Information about the operating system includes, for example, information about CPU and RAM usage, free space on disk partitions, load of network interfaces, a list of installed software, a list of open network connections, and a list of running processes. Part of this information may be confidential.

   - If you want to allow access only to general system information and information about the usage of RAM, CPU, and disk devices, add the following lines to the configuration file:

```
# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31
```

   - If you want to allow access to all system information, add the following lines to the configuration file:

```
view monitoring included .1
```

7. Specify the access mode and scope of information for the created user account. To do this, add the following lines to the configuration file:

```
rouser <user name> priv -V monitoring
```

8. To send SNMP traps, specify the IP address of the monitoring system and user credentials for receiving traps. To do this, add the following lines to the configuration file:

```
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <user name for receiving traps> -a <authentication algorithm> -A "
<user password for receiving traps>" -x <encryption algorithm> -X "<encryption password>" udp:<IP address>:162
```

The snmpd service is configured.

To integrate with multiple monitoring systems, create a separate user account for each system, specify the scope of available information for each user account (the 'view' and 'rouser' directives) and configure the sending of SNMP traps (the 'trapsess' directive).

### Starting the snmpd service with the new configuration

*To apply the new configuration:*

1. Restart the snmpd service:

```
systemctl restart snmpd
```

2. Check the status of the snmpd service:

```
systemctl status snmpd
```

The status must be `running`.

3. Allow the service to start automatically at operating system startup:

```
systemctl enable snmpd
```

4. If you are using a firewall in your operating system or network equipment, add rules to let SNMP packets through.

The snmpd service is running.

If the klcssnmp service was running at the time the snmpd service was configured, restart the klcssnmp service as well.

Checking the health of the snmpd service

To test the snmpd service, configure the use of SNMP in Kaspersky Security Center Linux and request SNMP data by using the snmpwalk utility.

*To get the scopes of SNMP data provided by Kaspersky Security Center Linux,*

run the following command:

```
snmpwalk -v3 -l authPriv -u <user name> -a <authentication algorithm> -A "<authentication password>" -x
<encryption algorithm> -X "<encryption password>" <IP address> .1.3.6.1.4.1.23668.1093.1
```

For example:

```
snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret"
127.0.0.1 .1.3.6.1.4.1.23668.1093.1
```

# Enabling and disabling notifying by SNMP

Kaspersky Security Center Linux sends notifications about Administration Server events in the form of SNMP traps.

By default, SNMP notifications for Kaspersky Security Center Linux events are disabled.

*To enable or disable notification by SNMP for Kaspersky Security Center Linux events:*

1. In the main menu, click the Administration Server name.

   The **Administration Server properties** window opens.

2. On the **Event configuration** tab of the properties window, click the event type for which you want to receive SNMP notifications.

3. In the pane that opens, enable or disable the **Notify by SNMP** toggle switch.

   This option is available only if the **Send statistics over SNMP** option is enabled.

SNMP notifications for Kaspersky Security Center Linux events are enabled or disabled according to your selection.

# Enabling and disabling SNMP in Kaspersky Security Center Linux

By default, sending statistics over SNMP is enabled. To send SNMP traps, configure the snmpd service.

*To enable or disable sending statistics over SNMP:*

1. In the main menu, click the Administration Server name.

   The **Administration Server properties** window opens.

2. On the **General** tab, select the **SNMP** section.

3. Enable or disable the **Send statistics over SNMP** toggle switch.

4. Click the **Save** button.

Sending statistics over SNMP is enabled or disabled according to your selection.

# Values of object identifiers for SNMP

The table below shows the values and descriptions of the objects identifiers (also referred to as OIDs), that are used for transferring information on Administration Server performance to third-party applications.

Values and descriptions of object identifiers for SNMP

| Value of object identifier | Numeric data type | OID | Description |
|---|---|---|---|
| `deploymentStatus` | `INTEGER { ok(0), info(1), warning(2), critical(3) }` | .1.3.6.1.4.1.23668.1093.1.1.1 | Deployment status. The status can be one of the following:<br>• **Info**. License is not valid for N devices anymore.<br>• **Warning**. One of the following:<br>There are M devices with Kaspersky applications installed on a total of N devices in Administration Server groups (N > M).<br>License L expires on N devices in M days.<br>Task T of installing applications has successfully finished on N devices, reboot is needed for M devices.<br>• **Critical** License expired for N devices.<br>• **OK**. None of the above. |
| `noAntivirusSoftware` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.1.2.1 | `deploymentStatus` shows that the Administration Server group contains too many devices without managed applications.<br>Value equals 1 if a few devices were found without managed applications, and 0 otherwise. |
| `remoteInstallTaskFailed` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.1.2.2 | `deploymentStatus` shows that the task of the remote installation has failed on some devices. The number of those devices can be obtained via `hostsRemoteInstallFailed`. |
| `licenceExpiring` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.1.2.3 | `deploymentStatus` shows that there are some devices with a license expiring in the next 7 days. The number of those devices can be obtained via `hostsLicenseExpiring`. |
| `licenceExpired` | `INTEGER { off(0), on(1) }` | .1.3.6.1.4.1.23668.1093.1.1.2.4 | `deploymentStatus` shows that there are some devices with an expired license. You can obtain the number of those devices via `hostsLicenseExpired`. |
| `hostsInGroups` | `Counter32` | .1.3.6.1.4.1.23668.1093.1.1.3 | Number of devices in Administration Server groups. |
| `hostsWithAntivirus` | `Counter32` | .1.3.6.1.4.1.23668.1093.1.1.4 | Number of devices in Administration Server groups with managed applications installed. |
| `hostsRemoteInstallFailed` | `Counter32` | .1.3.6.1.4.1.23668.1093.1.1.5 | Number of devices on which the task of the remote installation failed. |
| `licenceExpiringSerial` | `OCTET STRING` | .1.3.6.1.4.1.23668.1093.1.1.6 | ID of a license key that expires in less than 7 days. |
| `licenceExpiredSerial` | `OCTET STRING` | .1.3.6.1.4.1.23668.1093.1.1.7 | ID of the expired license key. |
| `licenceExpiringDays` | `Unsigned32` | .1.3.6.1.4.1.23668.1093.1.1.8 | Number of days before the license expires. For this parameter, the license period is considered expired if there are less than 7 days left until the expiration date.<br>If there are more than 7 days left until the expiration date, the value is 0. |

| Value of object identifier | Numeric data type | OID | Description |
|---|---|---|---|
| hostsLicenceExpiring | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.9 | Number of devices with a license that expires in less than 7 days. |
| hostsLicenceExpired | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.10 | Number of devices with an expired license. |
| updatesStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.2.1 | Current status of anti-virus bases update. The status can be one of the following:<br>• **Info**. Anti-virus bases on Administration Server or on the devices have not been updated in more than 1 day, and less than 1 day has passed since application installation.<br>• **Warning**. Anti-virus bases on Administration Server or on the devices have not been updated in more than 3 days. This value can be changed in group settings.<br>• **Critical** Anti-virus bases on Administration Server or on the devices have not been updated in more than 7 days. This value can be changed in group settings.<br>• **OK**. None of the above. |
| serverNotUpdated | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.2.2.1 | Administration Server has not been updated for a long time. The amount of time considered long is specified in updatesStatus. |
| notUpdatedHosts | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.2.2.2 | Some devices have not been updated for a long time (by default, 7 days or more for **Critical**, and 3 days for **Warning**). You can obtain the number of those devices via hostsNotUpdated. |
| lastServerUpdateTime | Hex-STRING | .1.3.6.1.4.1.23668.1093.1.2.3 | Last time when anti-virus bases were updated on Administration Server. |
| hostsNotUpdated | Counter32 | .1.3.6.1.4.1.23668.1093.1.2.4 | Number of devices containing anti-virus bases that have not been updated for a long time (by default, 7 days or more for **Critical**, and 3 days for **Warning**). If there are devices with the **Critical** update status, only these devices are counted. You can obtain the update status via updatesStatus. |
| protectionStatus | INTEGER { ok(0), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.3.1 | Status of real-time protection. One of the following:<br>• **Warning**. One of the following:<br>A security breach is detected on a device that belongs to the Administration Server group.<br>Encryption errors made some devices change protection status.<br>Full scan has not been performed for a long time.<br>• **Critical** Anti-virus protection is not working on some devices in Administration Server groups.<br>• **OK**. None of the above. |
| antivirusNotRunning | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.1 | A security application is not running on some devices. You can obtain the number of those devices via hostsAntivirusNotRunning. |
| realtimeNotRunning | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.2 | Real-time protection is not running on some devices. You can obtain the number of those devices via hostsRealtimeNotRunning. |
| psRealtimeLevelChanged | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.3 | The protection level during runtime differs from the level set by the administrator on N computers in administration groups. |
| notCuredFound | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.4 | There are devices containing non-disinfected objects. You can obtain the number of those devices via hostsNotCuredObject. |
| tooManyThreats | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.5 | There are threats found on some devices. You can obtain the number of those devices via hostsTooManyThreats. |

| Value of object identifier | Numeric data type | OID | Description |
|---|---|---|---|
| virusOutbreak | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.6 | The virus outbreak status of the system.<br>Value equals 1 if a certain amount of viruses were found during a certain amount of time, and 0 otherwise. Amount of viruses and amount of time are specified on Administration Server, by using the Virus attack settings. |
| psVulnerabilitiesFound | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.7 | Vulnerabilities were detected. |
| psEncryptionFaultsFound | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.8 | Encryption errors that changed the device protection status were detected. |
| psVulnerableHostsFound | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.9 | Vulnerabilities were detected on some devices. |
| psNotScannedLately | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.10 | Devices without a full scan for an extended period were detected. |
| psNagentsNotRunningUntilReboot | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.11 | Devices where the Network Agent starts only after a restart were detected. |
| hostsAntivirusNotRunning | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.3 | Number of devices with security applications not running. |
| hostsRealtimeNotRunning | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.4 | Number of devices with real-time protection not running. |
| hostsRealtimeLevelChanged | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.5 | Number of devices with real-time protection level not acceptable. |
| hostsNotCuredObject | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.6 | Number of devices containing non-disinfected objects. |
| hostsTooManyThreats | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.7 | Number of devices containing threats. |
| fullscanStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.4.1 | Status of anti-virus full scan is one of the following:<br>• **Info**. Less 7 days have passed since the moment of application installation.<br>• **Warning**. Anti-virus full scan hasn't been performed for more than 7 days since the moment of application installation.<br>• **Critical** Anti-virus full scan hasn't been performed for more than 14 days since the moment of application installation.<br>• **OK**. None of the above. |
| notScannedLately | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.4.2.1 | Some devices have not been scanned for a certain amount of time. You can obtain the number of those devices via hostsNotScannedLately. The amount of time is specified in fullScanStatus. |
| hostsNotScannedLately | Counter32 | .1.3.6.1.4.1.23668.1093.1.4.3 | Number of devices that have not been scanned for a certain amount of time. The amount of time is specified in fullScanStatus. |
| logicalNetworkStatus | INTEGER { ok(0), warning(1), critical(2) } | .1.3.6.1.4.1.23668.1093.1.5.1 | Status of the logical network of Administration Server. One of the following:<br>• **Warning**. If there are devices with a warning status that can't be accessed or if there are devices that do not belong to any Administration Server group.<br>• **Critical** If there are devices whose control has been lost by Administration Server, or if there are devices with a critical status and that cannot be accessed.<br>• **OK**. None of the above. |

| Value of object identifier | Numeric data type | OID | Description |
|---|---|---|---|
| notConnectedLongTime | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.5.2.1 | Some devices have not been connected to Administration Server for a long time (7 days or more for a device of **Warning** status and 4 days for a device of **Critical** status). You can obtain the number of those devices via hostsNotConnectedLongTime. |
| controlLost | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.5.2.2 | There are devices whose control has been lost by Administration Server. You can obtain the number of those devices via hostsControlLost. |
| hostsFound | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.3 | Number of devices found by Administration Server that do not belong to any Administration Server group. |
| groupsCount | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.4 | Number of groups at Administration Server. |
| hostsNotConnectedLongTime | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.5 | Number of devices that have not been connected to Administration Server for a long time. The amount of time considered long is specified in notConnectedLongTime. |
| hostsControlLost | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.6 | Number of devices that are not controlled by Administration Server. |
| eventsStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.6.1 | Status of the events subsystem is one of the following:<br>• **Warning**. One of the following:<br>Devices of Administration Server group have not been searching for Windows updates for a long time.<br>There are devices with status problems.<br>• **Critical** One of the following:<br>There is a "Critical" event on at least one device.<br>There is an "Error" event on at least one device.<br>There is an event of a task completing unsuccessfully on at least one device.<br>Devices of Administration Server group have not been searching for Windows updates for a long time.<br>There are devices with status problems.<br>• **Info** One of the following:<br>Less than a week has passed since the last full virus scan on all devices.<br>Remote installation tasks have completed and no devices require a restart.<br>Less than a week has passed since the last Administration Server update.<br>The Administration Server has not been updated for a long time, but an update is currently in progress.<br>• **OK**. None of the above. |
| criticalEventOccured | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.6.2.1 | eventsStatus shows that there are some critical events on Administration Server. You can obtain the number of those events via criticalEventsCount.<br>Value equals 1 if there is at least one critical event on any device, and 0 otherwise. |
| criticalEventsCount | Counter32 | .1.3.6.1.4.1.23668.1093.1.6.3 | Number of critical events on Administration Server. |

# Working with Kaspersky Security Center Linux under Kaspersky Next XDR Optimum license

If you purchased a license for Kaspersky Next XDR Optimum as part of an EPP application license and a Kaspersky Security Center Linux license, you will be able to use the Kaspersky Next XDR Optimum functionality after performing initial setup.

If you purchased a license for Kaspersky Next XDR Optimum separately as an extension of a previously purchased license after installing and activating Kaspersky applications on devices, you must reactivate Kaspersky Security Center Linux on the devices by using the new activation code or key file depending on the way you purchased the license for Kaspersky Next XDR Optimum. After that, you can perform initial setup.

Also, you can use the functionality of Kaspersky Next XDR Optimum in the test mode. To do this, you must first add a secondary physical Administration Server, and then activate this Server under your trial Kaspersky Next XDR Optimum license. The Kaspersky Next XDR Optimum functionality will be available on the secondary Server during the term of your trial license.

After you have activated the Administration Server under your Kaspersky Next XDR Optimum license, and deployed the license key to the devices managed by the relevant Administration Server, you can do the following:

- Respond to threats by using integrations with Kaspersky Automated Security Awareness Platform, Kaspersky Threat Intelligence Portal Sandbox, and Active Directory.
- Group alerts by attributes.

For more information about the features enabled by the Kaspersky Next XDR Optimum license, refer to the Kaspersky Endpoint Detection and Response Optimum Help.

## Integrations for responding to alerts

If you have the Kaspersky Next XDR Optimum license, you can configure integrations with the following solutions for responding to threats:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

These integrations are available if you activated Administration Server under a Kaspersky Next XDR Optimum license.
To perform response actions, you have to deploy the Kaspersky Next XDR Optimum license key to your managed applications.
When using the Kaspersky Next XDR Optimum functionality under a trial license, you must first add a secondary physical Administration Server, activate this secondary Administration Server under the trial license, and then deploy the license key to your devices managed by this Administration Server.

If you are using the Kaspersky Next EDR Optimum license, you do not have to activate the applications installed on your managed devices under the Kaspersky Next XDR Optimum license. You must do it only for new devices, if any.

Because the Kaspersky Next XDR Optimum license supports multitenancy, you can centrally distribute the license key to managed applications. Automatic distribution of the license to secondary and virtual Administration Servers is not supported.

To configure the integrations, you must have the **Read** and **Write** rights for the **General features: Application integration** functional area.

# Configuring integration with Active Directory for performing response actions

Integration with Active Directory enables you to perform response actions for Active Directory users affected by or involved in the alert.

To configure the integration with Active Directory for responding to alerts, you must use Kaspersky Security Center Linux Administration Server version 15.4 or later.

The integration with Active Directory for responding to alerts, and the settings for scanning the Active Directory domain controller (the address and user credentials of the domain controller) you specify when configuring a domain controller polling, are two different settings. Since you need to ensure that the user for whom a response action is to be performed has an Active Directory account, you must configure both the integrations: for scanning and for responding. The order is not significant.

The integration settings are not inherited and are applied only to the Administration Server (physical or virtual) on which you configure these settings.

*To configure integration with Active Directory for responding to alerts:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens with the **General** tab selected.

2. Do one of the following:

   - Select the **Distribution points** section, click the name of the required distribution point, and then in the properties window that opens, select the **Active Directory** section.
   - Select the **Active Directory response** section.

3. In the right pane, enable the **Active Directory integration** toggle switch.

   Later, if you want to turn off the integration, you can only do it for all connections by disabling the **Active Directory integration** toggle switch. You cannot turn off the integration for a separate connection. Instead, you can delete the connection.

   When you enable or disable the **Active Directory integration** toggle switch, the setting is applied for both the **Active Directory response** and the **Distribution points** sections.

4. Create a connection to the Active Directory domain controller by clicking the **Add** button.

5. In the window that opens, specify the following parameters for the connection:

   - **Domain controller address**

     Computer name, for example: `server.mycompany.com`.

     You can specify several addresses. All domain controllers whose addresses you specify must belong to the same domain.

   - **Active Directory domain name**

     DNS fully qualified domain name, for example: `mycompany.com`

     Also, you can specify SAM or NetBIOS name, for example: `mycompany`

     Use lowercase letters. If you create several connections for the Administration Server or a distribution point, specify different names for each connection.

     > To perform response actions, the Active Directory domain name that you specify in this field must match the Active Directory domain name specified in the alert.

   - **Login**

     Login of the Active Directory account with administrator rights under which the response actions are to be performed.

   - **Password**

     Password of the Active Directory account with administrator rights under which the response actions are to be performed.

6. If you want to check the connection status, click the **Check connection** button.

   If the connection is successfully established, the **Connected** status is displayed. Otherwise, the status is **Failed**, and an error message is displayed with the domain controllers to which you failed to connect.

   > You must take into account how the connection to Active Directory is made: **from a Linux device or from a Windows device**.

### Connecting from a Linux device

By default, when connecting and authenticating to a domain controller from a Linux device, the logic is the following:

1. Administration Server or a distribution point attempts to connect to the domain controller over LDAPS.

   The strong verification of the LDAP server certificate is performed.

2. You place the public part of the domain controller certificate into the system certificate repository to validate the certificate.

   The OS-dependent path to the system certificate authority (CA) is used to access the certificate chain.

For example:

- /etc/ssl/certs/ca-certificates.crt—Path for Debian-based operating systems (Debian, Ubuntu, Astra).
- /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem—Path for CentOS or Red Hat.

3. If the LDAPS connection fails, an error occurs, and no other connection protocol is used.

> In case of issues with LDAPS, you can contact Kaspersky Technical Support.

If you do not want to install the certificate into the system certificate repository, you can use the KLNAG_LDAP_SSL_CACERT flag to set the path to the domain controller certificate. To do it, run the command:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

where `</path/to/domain-controller/cert>` is the path to the public part of the domain controller certificate.

For example, if the path is `"/var/opt/kaspersky/ldap_cert.crt"`, the command is `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Connecting from a Windows device

When connecting and authenticating to a domain controller from a Windows device, the connection settings are defined by the domain.

You only have to ensure that:

- LDAPS is enabled and port 636 is available on the device.
- You allow connections to the domain controller through a firewall or a proxy server.

7. Click **Save**.

The window is closed, and the connection is displayed in the table of connections.

In the table of connections, you can do the following:

- Edit connection parameters.

  To do this, click the link with the **Domain controller address** parameter for the required connection. In the window that opens, change the required settings, and then click the **Save** button.

  You can edit only the **Login** and **Password** parameters.

- Delete connections.

  To do this, select the check box next to the connection you want to delete, click the **Remove** button in the toolbar, and then confirm the deletion of the connection.

# Configuring integration with Kaspersky Automated Security Awareness Platform

Integration with Kaspersky Automated Security Awareness Platform (hereinafter also referred to as KASAP) enables you to assign KASAP learning courses to users who are associated with alerts.

The integration settings are not inherited and are applied only to the Administration Server (physical or virtual) on which you configure these settings.

Before configuring an integration in Kaspersky Security Center Web Console, you have to create an authorization token and obtain a URL for API requests in KASAP.

*To configure integration with Kaspersky Automated Security Awareness Platform:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens with the **General** tab selected.

2. Select the **KASAP** section.

3. In the right pane, enable the **KASAP integration** toggle switch.

4. Specify the settings to be used for connection to KASAP:

   - **API token**—Token that you created to access KASAP Open API.
   - **URL**—URL for API requests that you obtained when creating the API token.
   - **Use a proxy server**—Toggle switch that enables the use of a proxy server when connecting to KASAP.

     The toggle switch is turned off by default.

5. If necessary, verify the settings you specified by clicking the **Check connection** button.

   The connection status is displayed.

6. Click the **Save** button.

The integration with Kaspersky Automated Security Awareness Platform is configured.

After the KASAP integration settings are saved, you can view the list of KASAP learning groups by clicking the **View groups** button.

If necessary, when the group list is displayed, you can update it by clicking the **Refresh groups** button.

You cannot hide the list after you open it. If you disable the **KASAP integration** toggle switch, the list of KASAP groups is not displayed.

# Configuring integration with Kaspersky Threat Intelligence Portal Sandbox

Integration with Kaspersky Threat Intelligence Portal (hereinafter also referred to as Kaspersky TIP) enables you to execute the files moved to the **Quarantine** section by using Kaspersky Sandbox—a safe environment isolated from your corporate network.

The integration settings are not inherited and are applied only to the Administration Server (physical or virtual) on which you configure these settings.

Before configuring integration, you have to obtain an authorization token for API requests on Kaspersky TIP.

*To configure integration with Kaspersky TIP Sandbox:*

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens with the **General** tab selected.

2. Select **Kaspersky TIP**.

3. In the right pane, enable the **Integration** toggle switch.

   The settings for connection to Kaspersky TIP are displayed.

   If after configuring and saving the integration settings you disable the **Integration** toggle switch, the settings are not deleted but the response cannot be performed.

4. Click the **Add token** button, and in the displayed window, specify the token previously obtained from Kaspersky TIP, then click the **Add** button.

   The window closes, and the API token is added.

5. If you want to use a proxy server when connecting to Kaspersky TIP, enable the **Use a proxy server** toggle switch.

   The toggle switch is turned off by default.

6. Click the **Save** button.

The integration with Kaspersky TIP Sandbox is configured.

Now, you can send files from the **Quarantine** section to Kaspersky TIP Sandbox for threat analysis. Maximum size of a file is 100 MB.

Because the Kaspersky Next XDR Optimum license supports multitenancy, files placed in **Quarantine** are divided by tenants. This tenant-level separation also applies when sending files to the Kaspersky TIP Sandbox and viewing the results if the administrator uses a dedicated TIP account and an API token related to each tenant. However, centralized management of the **Quarantine** section for all tenants is not possible, as the quarantine list does not display objects according to the server hierarchy.

# Grouping alerts by attributes

Alerts aggregation helps identify alerts that may be related to the same incident, simplifying the investigation process.

To enable the functionality of alert aggregation, you have to do the following:

- Enable the **Alerts** subsection in the main menu.
- Activate Administration Server under a Kaspersky Next XDR Optimum license, and then deploy the Kaspersky Next XDR Optimum license key to your managed applications.

  When using a Kaspersky Next XDR Optimum functionality under a trial license in the test mode, you must first add a secondary physical Administration Server, and then activate this server under this license.

If you are using the Kaspersky Next EDR Optimum license, you do not have to activate the applications installed on your managed devices under the Kaspersky Next XDR Optimum license. You must do it only for new devices, if any. Because the Kaspersky Next XDR Optimum license supports multitenancy, you can centrally distribute the license key to managed applications. Automatic distribution of the license to secondary and virtual Administration Servers is not supported.

You can aggregate alerts by device name, account, or hash name (SHA256).

> Alerts are aggregated by an attribute only if that attribute is not empty.

Alerts are aggregated together if they share at least one attribute and occur within 24 hours of any other alert in the group.

*To aggregate alerts by attributes:*

1. In the main menu, go to **Monitoring** → **Alerts**.
2. Do one of the following:
   - Enable the **Alerts aggregation** toggle switch, then select one or more attributes to aggregate alerts by:
     - **Device name**
     - **Account**
     - **File hash (SHA256)**

     The **Device name** and **Account** attributes are selected by default.
   - Click the settings icon ( ⚙ ). In the **Table settings** pane that opens, go to the **Grouping** tab. Select **Aggregation group ID** and click **Apply**.

When aggregation is enabled, alerts are sorted by **Event time** from newest to oldest. Additional sorting options are not supported. Selecting a different grouping option will disable aggregation.

The table displays alerts aggregated by attributes. Unaggregated alerts are displayed at the bottom of the table.

Each alert is assigned to only one group after aggregation.

# Integration between Kaspersky Security Center Web Console and other Kaspersky solutions

This section describes how to configure access from Kaspersky Security Center Web Console to another Kaspersky application, such as Kaspersky Managed Detection and Response. Also this section describes how to configure export to SIEM systems.

## Establishing a background connection

In order to configure interaction between Kaspersky Security Center Linux and another Kaspersky application or solution, for example, Kaspersky Managed Detection and Response (also referred to as MDR), you have to establish a background connection between Kaspersky Security Center Web Console and Administration Server. You can establish this connection only if your account has the Modify object ACLs right of the **General features: User permissions** functional area.

> You can configure interaction only between Kaspersky Managed Detection and Response and Windows-based version of Kaspersky Security Center.

*To establish a background connection:*

1. In the main menu, go to the **Settings** → **Integration**.
2. Select the **Web Console proxy server settings** tab.
3. In the **Integration** section, set the background connection toggle switch to **Background connection for integration Enabled**.
4. In the opened **Enable a background connection** section, click the **OK** button.

The background connection between Kaspersky Security Center Web Console and Administration Server is established. Administration Server creates an account for the background connection and this account is used as a service account to maintain interaction between Kaspersky Security Center Linux and another Kaspersky application or solution. The name of this service account contains the NWCSvcUser prefix. Administration Server automatically changes the password of the service account once every 30 days, for security reasons. You cannot delete the service account manually. Administration Server deletes this account automatically when you disable a cross-service connection. Administration Server creates a single service account for each Kaspersky Security Center Web Console and Administration Console and assigns all the service accounts to the security group with the name ServiceNwcGroup. Administration Server creates this security group automatically during the Kaspersky Security Center Linux installation process. You cannot delete this security group manually.

# Configuring proxy server connection

*To configure a proxy server connection for the Kaspersky Security Center Web Console and web plug-ins:*

1. In the main menu, go to **Settings** → **Integration**.
2. Select the **Web Console proxy server settings** tab.
3. Enable the **Use proxy server** option.
4. Specify the proxy server connection settings:
   - **Address of the proxy server**
   - **Port number**
   - **Proxy server authentication**
   - **User name** (required if you enable the **Proxy server authentication** option)
   - **Password** (required if you enable the **Proxy server authentication** option)
5. Click **Save** to save proxy server connection settings

If you have a hierarchy of Administration Servers, proxy server connection settings are not propagated to Web Consoles that manage secondary Administration Servers. You must configure proxy server connection separately for each Kaspersky Security Center Web Console.

# Remote diagnostics of client devices

You can use remote diagnostics for remote execution of the following operations on Windows-based and Linux-based client devices:

- Enabling and disabling tracing, changing the tracing level, and downloading the trace file
- Downloading system information and application settings
- Downloading event logs
- Generating a dump file for an application
- Starting diagnostics and downloading diagnostics reports
- Starting, stopping, and restarting applications

You can use event logs and diagnostics reports downloaded from a client device to troubleshoot problems on your own. Also, if you contact Kaspersky Technical Support, a Technical Support specialist might ask you to download trace files, dump files, event logs, and diagnostics reports from a client device for further analysis at Kaspersky.

# Opening the remote diagnostics window

To perform remote diagnostics on Windows-based and Linux-based client devices, you first have to open the remote diagnostics window.

*To open the remote diagnostics window:*

1. To select the device for which you want to open the remote diagnostics window, perform one of the following:
   - If the device belongs to an administration group, in the main menu, go to **Asset management** → **Managed devices**.
   - If the device belongs to the Unassigned devices group, in the main menu, go to **Asset management** → **Unassigned devices**.
2. Click the name of the required device.
3. In the device properties window that opens, select the **Advanced** tab.
4. On the **Advanced** tab, click **Remote diagnostics**.

   This opens the **Remote diagnostics** window of a client device. If connection between Administration Server and the client device is not established, the error message displays.

Alternatively, if you need to obtain all diagnostic information about a Linux-based client device at once, you can run the collect.sh script on this device.

# Enabling and disabling tracing for applications

You can enable and disable tracing for applications, including Xperf tracing.

## Enabling and disabling tracing

*To enable or disable tracing on a remote device:*

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the **Kaspersky applications** tab.

   In the **Application management** section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select the application for which you want to enable or disable tracing.

   The list of remote diagnostics options opens.
4. If you want to enable tracing:

   a. In the **Tracing** section, click **Enable tracing**.

   b. In the **Modify tracing level** window that opens, we recommend that you keep the default values of the settings. When required, a Technical Support specialist will guide you through the configuration process. The following options are available:

   - **Tracing level**

     The tracing level defines the amount of detail that the trace file contains.

   - **Rotation-based tracing**

     The application overwrites the tracing information to prevent excessive increase in the size of the trace file. Specify the maximum number of files to be used to store the tracing information, and the maximum size of each file. If the maximum number of trace files of the maximum size are written, the oldest trace file is deleted so that a new trace file can be written.

     This setting is available for Kaspersky Endpoint Security only.

   c. Click the **Save** button.

   The tracing is enabled for the selected application. In some cases, the security application and its task must be restarted in order to enable tracing.

   > On Linux-based client devices, tracing for the Updater of Network Agent component is regulated by the Network Agent settings. Therefore, the **Enable tracing** and **Modify tracing level** options are disabled for this component on client devices running Linux.

5. If you want to disable tracing for the selected application, click the **Disable tracing** button.

   The tracing is disabled for the selected application.

## Enabling Xperf tracing

For Kaspersky Endpoint Security, a Technical Support specialist may ask you to enable Xperf tracing for information about the system performance.

*To enable and configure Xperf tracing or disable it:*

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the **Kaspersky applications** tab.

   In the **Application management** section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select Kaspersky Endpoint Security for Windows.

   The list of remote diagnostics options for Kaspersky Endpoint Security for Windows displays.
4. In the **Xperf tracing** section, click **Enable Xperf tracing**.

   If Xperf tracing is already enabled, the **Disable Xperf tracing** button is displayed instead. Click this button if you want to disable Xperf tracing for Kaspersky Endpoint Security for Windows.
5. In the **Change Xperf tracing level** window that opens, depending on the request from the Technical Support specialist, do the following:

   a. Select one of the following tracing levels:

   - **Light level**

     A trace file of this type contains the minimum amount of information about the system.

     By default, this option is selected.

   - **Deep level**

     A trace file of this type contains more detailed information than trace files of the *Light* type and may be requested by Technical Support specialists when a trace file of the *Light* type is not enough for the performance evaluation. A *Deep* trace file contains technical information about the system including information about hardware, operating system, list of started and finished processes and applications, events used for performance evaluation, and events from Windows System Assessment Tool.

   b. Select one of the following Xperf tracing types:

   - **Basic type**

     The tracing information is received during operation of the Kaspersky Endpoint Security application.

     By default, this option is selected.

   - **On-restart type**

     The tracing information is received when the operating system starts on the managed device. This tracing type is effective when the issue that affects the system performance occurs after the device is turned on and before Kaspersky Endpoint Security starts.

   You may also be asked to enable the **Rotation file size, in MB** option to prevent excessive increase in the size of the trace file. Then specify the maximum size of the trace file. When the file reaches the maximum size, the oldest tracing information is overwritten with new information.

c. Define the rotation file size.

d. Click the **Save** button.

Xperf tracing is enabled and configured.

6. If you want to disable Xperf tracing for Kaspersky Endpoint Security for Windows, click **Disable Xperf tracing** in the **Xperf tracing** section.

   Xperf tracing is disabled.

# Downloading trace files of an application

*To download a trace file of an application:*

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the **Kaspersky applications** tab.

   In the **Application management** section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select the application for which you want to download a trace file.
4. In the **Tracing** section, click the **Trace files** button.

   This opens the **Device tracing logs** window, where a list of trace files is displayed.
5. In the list of trace files, select the file that you want to download.
6. Do one of the following:

   - Download the selected file by clicking **Download**. You can select one or several files for downloading.
   - Download a portion of the selected file:

     a. Click **Download a portion**.

     You cannot download portions of several files at the same time. If you select more than one trace file, the **Download a portion** button will be disabled.

     b. In the window that opens, specify the name and the file portion to download, according to your needs.

     For Linux-based devices, editing the file portion name is not available.

     c. Click **Download**.

The selected file, or its portion, is downloaded to the location that you specify.

# Deleting trace files

You can delete trace files that are no longer needed.

*To delete a trace file:*

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window that opens, select the **Event logs** tab.
3. In the **Trace files** section, click **Windows Update logs** or **Remote installation logs**, depending on which trace files you want to delete.

   The **Windows Update logs** link is available only for Windows-based client devices.

   This opens the **Device tracing logs** window, where a list of trace files is displayed.
4. In the list of trace files, select one or several files that you want to delete.
5. Click the **Remove** button.

The selected trace files are deleted.

# Downloading application settings

*To download application settings from a client device:*

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the **Kaspersky applications** tab.
3. In the **Application settings** section, click the **Download** button to download information about the settings of the applications installed on the client device.

The ZIP archive with information is downloaded to the specified location.

# Downloading system information from a client device

*To download system information from a client device:*

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the **System information** tab.
3. Click the **Download** button to download the system information about the client device.

   If you obtain system information about a Linux-based device, a dump file for emergency terminated applications is added to the resulting file.

   The archive may contain sensitive data (for example, keys and passwords) in plain text. We recommend that you review the files in the archive and remove such data before sending it to Kaspersky Technical Support.

The file with information is downloaded to the specified location.

# Downloading event logs

*To download an event log from a remote device:*

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, on the **Event logs** tab, click **All device logs**.
3. In the **All device logs** window, select one or several relevant logs.
4. Do one of the following:
   - Download the selected log by clicking **Download entire file**.
   - Download a portion of the selected log:
     a. Click **Download a portion**.
     You cannot download portions of several logs at the same time. If you select more than one event log, the **Download a portion** button will be disabled.
     b. In the window that opens, specify the name and the log portion to download, according to your needs.
     For Linux-based devices, editing the log portion name is not available.
     c. Click **Download**.

The selected event log, or a portion of it, is downloaded to the specified location.

# Starting, stopping, restarting the application

You can start, stop, and restart applications on a client device.

*To start, stop, or restart an application:*

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the **Kaspersky applications** tab.
   In the **Application management** section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select the application that you want to start, stop, or restart.
4. Select an action by clicking one of the following buttons:
   - **Stop application**
     This button is available only if the application is currently running.
   - **Restart application**
     This button is available only if the application is currently running.

- **Start application**

  This button is available only if the application is not currently running.

Depending on the action that you have selected, the required application is started, stopped, or restarted on the client device.

If you restart the Network Agent, a message is displayed stating that the current connection of the device to the Administration Server will be lost.

# Running the remote diagnostics of Kaspersky Security Center Linux Network Agent and downloading the results

*To start diagnostics for Kaspersky Security Center Linux Network Agent on a remote device and download the results:*

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the **Kaspersky applications** tab.

   In the **Application management** section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select **Kaspersky Security Center Linux Network Agent**.

   The list of remote diagnostics options opens.
4. In the **Diagnostics report** section, click the **Run diagnostics** button.

   This starts the remote diagnostics process and generates a diagnostics report. When the diagnostics process is complete, the **Download diagnostics report** button becomes available.
5. Click the **Download diagnostics report** button to download the report.

The report is downloaded to the specified location.

# Running an application on a client device

You may have to run an application on the client device, if a Kaspersky support specialist requests it. You do not have to install the application on that device.

If you want to run a custom script on the client device, you can use the `KLACDT_SAVE_SETTING` environment variable to determine the path where the execution results will be saved. For example:

- For a Windows-based device:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- For a Linux-based device:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

*To run an application on the client device:*

1. Open the remote diagnostics window of a client device.
2. In the remote diagnostics window, select the **Running a remote application** tab.
3. In the **Object type** field, select the type of object that you want to upload:
   - Select **File** to upload the executable file.
   - Select **Folder** to upload the folder containing the application that you want to run on the client device.

     If you select this object type, the **Name of the executable file to be run** field appears. In this field, specify the name of the executable file in the folder. You can also specify the relative path to the file.
   - Select **Archive** to upload the ZIP archive containing the application that you want to run on the client device.

     If you select this object type, the **Name of the executable file to be run** field appears. In this field, specify the name of the executable file in the folder. You can also specify the relative path to the file.

     > The ZIP archive must include the utility folder. This folder contains the executable file to be run on a remote device.
4. Upload the object by selecting it in the system window, or dragging it to the upload field.
5. If necessary, in the **Command line arguments** field, specify the command line arguments to be passed when running the executable file.
6. Click the **Upload and run** button to run the selected application on a client device.
7. After the application execution is completed successfully, download the execution results by clicking the **Download application execution results** button.

   > The application execution results are stored until you run a new diagnostic or close the window.

Remote diagnostics of the client device by using the application is completed.

# Running remote diagnostics on a Linux-based client device

Kaspersky Security Center Linux allows you to download the basic diagnostic information from a client device. Alternatively, you can obtain the diagnostic information about a Linux-based device by using the collect.sh script by Kaspersky. This script must be run on the Linux client device that needs to be diagnosed. A file is then created with diagnostic information, system information for the device, application trace files, device event logs and a dump file for crashes and terminated processes.

We recommend that you use the collect.sh script to obtain all diagnostic information about the Linux-based client device at once. If you download the diagnostic information remotely through Kaspersky Security Center Linux, you will need to go through all sections of the remote diagnostics interface. Also the diagnostic information for a Linux-based device will probably not be obtained completely.

If you need to send the generated file with the diagnostic information to the Kaspersky Technical Support, delete all confidential information before sending the file.

*To download the diagnostic information from a Linux-based client device by using the collect.sh script:*

1. Download the collect.sh script packed in the collect.tar.gz archive.
2. Copy the downloaded archive to the Linux-based client device that needs to be diagnosed.
3. Run the following command to unpack the collect.tar.gz archive:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Run the following command to specify the script execution rights:

   ```
   # chmod +x collect.sh
   ```

5. Run the collect.sh script by using an account with administrator rights:

   ```
   # ./collect.sh
   ```

A file with the diagnostic information is generated and saved to the /tmp/$HOST_NAME-collect.tar.gz folder.

# Managing third-party applications and executable files on client devices

This section describes the features of Kaspersky Security Center Linux related to the management of third-party applications and executable files run on client devices.

## Using Application Control to manage executable files

You can use the Application Control component to allow or block startup of executable files on user devices. The Application Control component supports Windows-based and Linux-based operating systems.

> For Linux-based operating systems, Application Control component is available starting from Kaspersky Endpoint Security 11.2 for Linux.

### Prerequisites

- Kaspersky Security Center Linux is deployed in your organization.
- The policy of Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Windows is created and is active. The Application Control component is enabled in the policy.

### Stages

The Application Control usage scenario proceeds in stages:

1. **Forming and viewing the list of executable files on client devices**

   This stage helps you find out what executable files are found on managed devices. View the list of executable files and compare it with the lists of allowed and prohibited executable files. The restrictions on executable files usage can be related to the information security polices in your organization.

   How-to instructions: Obtaining and viewing a list of executable files stored on client devices

2. **Creating categories for executable files used in your organization**

   Analyze the lists of executable files stored on managed devices. Based on the analysis, create categories for executable files. It is recommended to create a "Work applications" category that covers the standard set of executable files that are used at your organization. If different security groups use their own sets of executable files in their work, a separate category can be created for each security group.

Startup of executable files whose settings do not match any of the Application Control rules is regulated by the selected operating mode of the component:

- *Denylist*. The mode is used if you want to allow the startup of all executable files except those specified in block rules. This mode is selected by default.
- *Allowlist*. The mode is used if you want to block the startup of all executable files except those specified in allow rules.

The Application Control rules are implemented through categories for executable files. In Kaspersky Security Center Linux there are three types of categories for executable files:

- Category with content added manually. You define conditions, for example, file metadata, file hashcode, file certificate, file path, to include executable files in the category.
- Category that includes executable files from selected devices. You specify a device whose executable files are automatically included in the category.
- Category that includes executable files from selected folder. You specify a folder from which executable files are automatically included in the category.

3. **Configuring Application Control in the Kaspersky Endpoint Security policy**

   Configure the Application Control component in Kaspersky Endpoint Security for Linux policy using the categories you have created on the previous stage.

   How-to instructions: Configuring Application Control in the Kaspersky Endpoint Security for Windows policy

4. **Turning on Application Control component in test mode**

   To ensure that Application Control rules do not block executable files required for user's work, it is recommended to enable testing of Application Control rules and analyze their operation after creating new rules. When testing is enabled, Kaspersky Endpoint Security for Windows will not block executable files whose startup is forbidden by Application Control rules, but will instead send notifications about their startup to the Administration Server.

   When testing Application Control rules, it is recommended to perform the following actions:

   - Determine the testing period. Testing period can vary from several days to two months.
   - Examine the events resulting from testing the operation of Application Control.

   How-to instructions for Kaspersky Security Center Web Console: Configuring Application Control component in the Kaspersky Endpoint Security for Windows policy. Follow this instruction and enable the **Test Mode** option in configuration process.

5. **Changing the settings of Application Control component**

   If necessary, make changes to the Application Control settings. Based on the test results, you can add executable files related to events of the Application Control component to a category with content added manually.

   How-to instructions: Kaspersky Security Center Web Console: Adding event-related executable files to the application category

6. **Applying the rules of Application Control in operation mode**

   After Application Control rules are tested and configuration of categories is complete, you can apply the rules of Application Control in operation mode.

   How-to instructions for Kaspersky Security Center Web Console: Configuring Application Control component in the Kaspersky Endpoint Security for Windows policy. Follow this instruction and disable the **Test Mode** option in configuration process.

7. **Verifying Application Control configuration**

   Be sure that you have done the following:

   - Created categories for executable files.
   - Configured Application Control using the categories.
   - Applied the rules of Application Control in operation mode.

### Results

When the scenario is complete, startup of executable files on managed devices is controlled. The users can run only those executable files that are allowed in your organization and cannot run executable files that are prohibited in your organization.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

# Obtaining and viewing a list of executable files stored on client devices

You can obtain the list of executable files stored on client devices in one of the following ways:

- Enabling notifications about applications startup in Kaspersky Endpoint Security policy.
- Creating an inventory task.

### Enabling notifications about applications startup in Kaspersky Endpoint Security policy

*To enable notifications about applications startup:*

1. Open the Kaspersky Endpoint Security policy settings, and then go to **General settings** → **Reports and Storage**.
2. In the **Data transfer to Administration Server** settings group, select the **About started applications** check box, and save the changes.

   When a user attempts to start executable files, information about these files is added to the list of executable files on a client device. Kaspersky Endpoint Security sends this information to Network Agent, and then Network Agent sends it to Administration Server.

## Creating an inventory task

For Kaspersky Endpoint Security for Linux, the feature of inventorying executable files is available since no earlier that version 11.2.

You can reduce load on the database while obtaining information about the installed applications. To save database space, run an inventory task on reference devices on which a standard set of software is installed. The preferable number of devices is 1-3.

*To create an inventory task for executable files on client devices:*

1. In the main menu, go to **Tasks**.

   The list of tasks is displayed.

2. Click **Add**.

   The New task wizard starts. Follow the steps of the wizard.

3. On the **New task settings** page, from the **Application** drop-down list, select Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Windows, depending on the operating system of the client devices.

4. From the **Task type** drop-down list, select **Inventory**.

5. On the **Finish task creation** page, click the **Finish** button.

   After the New task wizard has finished, the **Inventory** task is created and configured. If you want, you can change the settings for the created task. The newly created task is displayed in the list of tasks.

For a detailed description of the inventory task, see the Kaspersky Endpoint Security for Linux Help and the Kaspersky Endpoint Security for Windows Help.

After the **Inventory** task is performed, the list of executable files stored on managed devices is formed, and you can view the list.

During inventory, executable files in the following formats can be detected (depending on the option that you select in the inventory task properties): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, and HTML.

## Viewing the list of executable files stored on managed devices

*To view the list of executable files stored on client devices:*

In the main menu, go to **Software management** → **Third-party applications** → **Executable files**.

The page displays the list of executable files stored on client devices.

If necessary, you can send the executable file of the managed device to the device where your Kaspersky Security Center Web Console is open.

*To send an executable file:*

1. In the main menu, go to **Software management** → **Third-party applications** → **Executable files**.
2. Click the link of the executable file that you want to send.
3. In the window that opens, go to the **Devices** section, and then select the check box of the managed device from which you want to send the executable file.

   Before you send the executable file, make sure that the managed device has a direct connection to the Administration Server, by selecting the **Do not disconnect from the Administration Server** check box.

4. Click the **Send** button.

The selected executable file is downloaded for further sending to the device where your Kaspersky Security Center Web Console is open.

# Creating an application category with content added manually

You can specify a set of criteria as a template of executable files for which you want to allow or block a start in your organization. On the basis of executable files corresponding to the criteria, you can create an application category and use it in the Application Control component configuration.

*To create an application category with content added manually:*

1. In the main menu, go to **Software management** → **Third-party applications** → **Application categories**.

   The page with a list of application categories is displayed.

2. Click the **Add** button.

   The New category wizard starts. Proceed through the wizard by using the **Next** button.

3. On the **Select category creation method** step, specify the application category name and select the **Category with content added manually. Data of executable files is manually added to the category** option.
4. On the **Conditions** step, click the **Add** button to add a condition criterion to include files in the creating category.
5. On the **Condition criteria** step, do the following:

   a. Select a rule type for the creation of the category:

   - **From KL category**

     If this option is selected, you can specify a Kaspersky application category as the condition of adding applications to the user category. The applications from the specified Kaspersky category will be added to the user application category.

- **Select certificate from repository**

  If this option is selected, you can specify certificates from the repository. The category condition matches only the executable files signed by the specified certificate.

  Certificates are added to the repository if you created and started an inventory task or selected the **About started applications** check box in the Kaspersky Endpoint Security policy. You can perform both actions.

  > Information about certificates can be extracted only from executable files in PE format (.exe, .dll, .sys).

- **Specify path to application (masks supported)**

  If this option is selected, you can specify the path to the folder on the client device containing the executable files that are to be added to the user application category.

- **Removable drive**

  If this option is selected, you can specify the type of the medium (any drive or removable drive) on which the application is run. Applications that have been run on the selected drive type are added to the user application category.

- **Hash, metadata, or certificate**:

  - **Select from list of executable files**

    If this option is selected, you can use the list of executable files on the client device to select and add applications to the category.

  - **Select from applications registry**

    If this option is selected, application registry is displayed. After you select an application from the registry, the window opens with the parameters filled in with metadata from the application that you selected:

    - Name of the file.
    - File version. You can specify precise value of the version or describe a condition, for example "greater than 5.0".
    - Application name.
    - Application version. You can specify precise value of the version or describe a condition, for example "greater than 5.0".
    - Vendor.

    Note that only the launch of executable files that meet the specified parameters is blocked, not the launch of the application you select. If the selected application metadata matches the one of the executable file that is launched when you launch the application, then you can proceed to the next step. Otherwise, you have to change the values manually to match the metadata of the executable file.

  - **Specify manually**

If this option is selected, you must specify file hash, or metadata, or certificate as the condition of adding applications to the user category.

**File Hash**

Depending on the version of the security application installed on devices on your network, you should select an algorithm for hash value computing by Kaspersky Security Center Linux for files in this category. Information about hash values computed by hash functions is stored in the Administration Server database.

SHA256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security for Linux supports SHA256 computing.

Select either of the options of hash value computing by Kaspersky Security Center Linux for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security for Linux, select the **SHA256** check box.
- Select the **MD5 hash** check box only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support an MD5 hash function.

**Metadata**

If this option is selected, you can specify file metadata as file name, file version, vendor. The category condition matches only the executable files with the same metadata.

**Certificate**

If this option is selected, you can specify certificates from the repository. The category condition matches only the executable files signed by the specified certificate.

Certificates are added to the repository if you created and started an inventory task or selected the **About started applications** check box in the Kaspersky Endpoint Security policy. You can perform both actions.

- **From archived folder**

  If this option is selected, you can specify a file of an archived folder, and then select which condition you want to use to add applications to the user category. The archived folder is unpacked and the conditions that you select are applied to the files in the folder. As a condition, you can select one of the following criteria:

  - **File Hash**

    You select which hash function (MD5 or SHA256) you want to use to calculate hash values. The applications that have the same hash value as the files in the archived folder are added to the user application category.

    Select an MD5 hash function only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support an MD5 hash function.

  - **Metadata**

    You select which metadata you want to use as criteria. Executable files that contain the same metadata will be added to the user application category.

- **Certificate**

  You select which certificate properties (certificate subject, fingerprint, or issuer) you want to use as criteria. Executable files that have been signed with the certificates that have the same properties will be added to the user category.

> **Metadata** and **Certificate** criteria must be specified manually after uploading a file or an archived folder if you want to use these criteria.

If this option is selected, you can specify a file of an archived folder, and then select which condition you want to use to add applications to the user category. The archived folder is unpacked and the conditions that you select are applied to the files in the folder. As a condition, you can select one of the following criteria:

- **File Hash**

  You select which hash function (MD5 or SHA256) you want to use to calculate hash values. The applications that have the same hash value as the files in the archived folder are added to the user application category.

  Select an MD5 hash function only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support an MD5 hash function.

- **Metadata**

  You select which metadata you want to use as criteria. Executable files that contain the same metadata will be added to the user application category.

- **Certificate**

  You select which certificate properties (certificate subject, fingerprint, or issuer) you want to use as criteria. Executable files that have been signed with the certificates that have the same properties will be added to the user category.

> **Metadata** and **Certificate** criteria must be specified manually after uploading a file or an archived folder if you want to use these criteria.

b. If necessary, add a comment in the **Description** field. The number of symbols cannot exceed 1000.

Later you will be able to edit or delete the comment. To do so, in the application category properties, open the **Conditions** tab, then in the **Condition criterion** column, click the link with the condition for which you want to edit or delete the comment.

> When selecting the **From KL category** rule type, you can add one comment for all conditions to be created based on this rule type. You can edit or delete the comment for every condition separately.

The selected criterion is added to the list of conditions.

You can add as many criteria as you need for the application category that is being created.

6. On the **Exclusions** step, click the **Add** button to add an exclusive condition criterion to exclude files from the category that is being created.

If necessary, you can add a comment in the **Description** field. The number of symbols cannot exceed 1000.

Later, you can edit or delete the comment To do so, in the application category properties, open the **Exclusions** tab, then in the **Condition criterion** column, click the link with the condition for which you want to edit or delete the comment.

7. On the **Condition criteria** step, select a rule type from the list, in the same way that you selected a rule type for category creation.

When the wizard finishes, the application category is created and displayed in the list of application categories. You can use the created application category when you configure Application Control.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

# Creating an application category that includes executable files from selected devices

You can use executable files from selected devices as a template of executable files that you want to allow or block. Based on executable files from selected devices, you can create an application category and use it in the Application Control component configuration.

Make sure that the following prerequisites are met:

- The Application Control component is enabled in the Kaspersky Endpoint Security policy.
- A list of executable files stored on managed devices has been obtained.

*To create application category that includes executable files from selected devices:*

1. In the main menu, go to **Software management** → **Third-party applications** → **Application categories**.

   The page with a list of categories of executable files is displayed.

2. Click the **Add** button.

   The New category wizard starts. Proceed through the wizard by using the **Next** button.

3. At the **Select category creation method** step, specify the category name and select the **Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category**.

4. Click **Add**.

5. In the window that opens, select a device or devices whose executable files will be used to create the application category.

6. Specify the following settings:

   - **Hash value computing algorithm**

     Depending on the version of the security application installed on devices on your network, you should select an algorithm for hash value computing by Kaspersky Security Center Linux for files in this category. Information about hash values computed by hash functions is stored in the Administration Server database.

     SHA256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security for Linux supports SHA256 computing.

Select either of the options of hash value computing by Kaspersky Security Center Linux for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security for Linux, select the **SHA256** check box.

Select the **MD5 hash** check box only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support an MD5 hash function.

The **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box is selected by default.

The **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** is cleared by default.

- **Synchronize data with Administration Server repository**

  Select this option if you want that Administration Server periodically to check changes in the specified folder (or folders).

  By default, this option is disabled.

  If you enable this option, specify the period (in hours) to check changes in the specified folder (folders). By default, scan interval is 24 hours.

- **File type**

  In this section, you can specify file type that is used to create the application category.

  **All files**. All files are taken into consideration when creating the category. By default, this option is selected.

  **Only files outside the application categories**. Only files outside the application categories are taken into consideration when creating the category.

- **Folders**

  In this section you can specify which folders from the selected device (devices) contain files that are used to create the application category.

  **All folders**. All folders are taken into consideration for the creating category. By default, this option is selected.

  **Specified folder**. Only specified folder is taken into consideration for the creating category. If you select this option you must specify path to the folder.

When the wizard finishes, the category of executable files is created. It is displayed in the list of categories. You can use the created category when you configure Application Control.

# Creating an application category that includes executable files from selected folder

You can use executable files from a selected folder as a standard of executable files that you want to allow or block in your organization. On the basis of executable files from the selected folder, you can create an application category and use it in the Application Control component configuration.

*To create a category that includes executable files from the selected folder:*

1. In the main menu, go to **Software management → Third-party applications → Application categories**.

   The page with a list of categories is displayed.

2. Click **Add**.

   The New category wizard starts. Proceed through the wizard by using the **Next** button.

3. On the **Select category creation method** step, specify the category name and select the **Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category** option.

4. Specify the folder whose executable files will be used to create the category.

5. Configure the following settings:

   - **Include dynamic-link libraries (DLL) in this category**

     The application category includes dynamic-link libraries (files in DLL format), and the Application Control component logs the actions of such libraries running in the system. Including DLL files in the category may lower the performance of Kaspersky Security Center Linux.

     This check box is cleared by default.

   - **Include script data in this category**

     The application category includes data on scripts, and scripts are not blocked by Web Threat Protection. Including the script data in the category may lower the performance of Kaspersky Security Center Linux.

     This check box is cleared by default.

   - **Hash value computing algorithm**: **Calculate SHA256 for files in this category** / **Calculate MD5 hashes for files in this category**

     Depending on the version of the security application installed on devices on your network, you should select an algorithm for hash value computing by Kaspersky Security Center Linux for files in this category. Information about hash values computed by hash functions is stored in the Administration Server database.

     SHA256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security for Linux supports SHA256 computing.

     Select either of the options of hash value computing by Kaspersky Security Center Linux for files in the category:

     - If all instances of security applications installed on your network are Kaspersky Endpoint Security for Linux, select the **SHA256** check box.

     Select the **MD5 hash** check box only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support an MD5 hash function.

     The **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box is selected by default.

     The **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** is cleared by default.

   - **Force folder scan for changes**

     If this option is enabled, the application regularly checks the folder of category content addition for changes. You can specify the frequency of checks (in hours) in the entry field next to the check box. By default, the time interval between forced checks is 24 hours.

If this option is disabled, the application does not force any checks of the folder. The Server attempts to access files if they have been modified, added, or deleted.

By default, this option is disabled.

When the wizard finishes, the category of executable files is created. It is displayed in the list of categories. You can use the category at Application Control configuration.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

# Viewing the list of application categories

You can view the list of configured categories of executable files and the settings of each category.

*To view the list of application categories,*

In the main menu, go to **Software management** → **Third-party applications** → **Application categories**.

The page with a list of categories is displayed.

*To view properties of an application category,*

Click the name of the category.

The properties window of the category is displayed. The properties are grouped on several tabs.

# Adding event-related executable files to the application category

After you configure Application Control in the Kaspersky Endpoint Security policies, the following events will be displayed in the list of events:

- **Application startup prohibited** (*Critical* event). This event is displayed if you have configured Application Control to apply rules.
- **Application startup prohibited in test mode** (*Info* event). This event is displayed if you have configured Application Control to test rules.
- **Message to administrator about application startup prohibition** (*Warning* event). This event is displayed if you have configured Application Control to apply rules and a user has requested access to the application that is blocked at startup.

It is recommended to create event selections to view events related to Application Control operation.

You can add executable files related to Application Control events to an existing application category or to a new application category. You can add executable files only to an application category with content added manually.

*To add executable files related to Application Control events to an application category:*

1. In the main menu, go to **Monitoring → Event selections**.

   The list of event selections is displayed.

2. Select the event selection to view events related to Application Control and start this event selection.

   If you have not created event selection related to Application Control, you can select and start a predefined selection, for example, **Recent events**.

   The list of events is displayed.

3. Select the events whose associated executable files you want to add to the application category, and then click the **Assign to category** button.

   The New category wizard starts. Proceed through the Wizard by using the **NEXT** button.

4. On the wizard page, specify the relevant settings:

   - In the **Action on executable file related to the event** section, select one of the following options:

     - **Add to a new application category**

       Select this option if you want to create a new application category based on event-related executable files.

       By default, this option is selected.

       If you have selected this option, specify a new category name.

     - **Add to an existing application category**

       Select this option if you want to add event-related executable files to an existing application category.

       By default, this option is not selected.

       If you have selected this option, select the application category with content added manually to which you want to add executable files.

   - In the **Rule type** section, select one of the following options:

     - **Rules for adding to inclusions**

     - **Rules for adding to exclusions**

   - In the **Parameter used as a condition** section, select one of the following options:

     - **Certificate details (or SHA256 hashes for files without a certificate)**

       Files may be signed with a certificate. Multiple files may be signed with the same certificate. For example, different versions of the same application may be signed with the same certificate, or several different applications from the same vendor may be signed with the same certificate. When you select a certificate, several versions of an application or several applications from the same vendor may end up in the category.

       Each file has its own unique SHA256 hash function. When you select an SHA256 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

       Select this option if you want to add to the category rules the certificate details of an executable file (or the SHA256 hash function for files without a certificate).

       By default, this option is selected.

- **Certificate details (files without a certificate will be skipped)**

  Files may be signed with a certificate. Multiple files may be signed with the same certificate. For example, different versions of the same application may be signed with the same certificate, or several different applications from the same vendor may be signed with the same certificate. When you select a certificate, several versions of an application or several applications from the same vendor may end up in the category.

  Select this option if you want to add the certificate details of an executable file to the category rules. If the executable file has no certificate, this file will be skipped. No information about this file will be added to the category.

- **Only SHA256 (files without a hash will be skipped)**

  Each file has its own unique SHA256 hash function. When you select an SHA256 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

  Select this option if you want to add only the details of the SHA256 hash function of the executable file.

- **Only MD5 hashes**

  Select this option only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support an MD5 hash function.

  Each file has its own unique MD5 hash function. When you select an MD5 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

5. Click the **OK** button.

   When the wizard finishes, executable files related to the Application Control events are added to the existing application category or to a new application category. You can view settings of the application category that you have modified or created.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

# Configuring Application Control in the Kaspersky Endpoint Security for Windows policy

After you create Application Control categories, you can use them for configuring Application Control in Kaspersky Endpoint Security for Windows policies.

*To configure Application Control in the Kaspersky Endpoint Security for Windows policy:*

1. In the main menu, go to **Asset management** → **Policies**.

   A page with a list of policies is displayed.

2. Click the **Kaspersky Endpoint Security for Windows** policy.

   The policy settings window opens.

3. Go to **Application settings** → **Security Controls** → **Application Control**.

   The **Application Control** window with Application Control settings is displayed.

4. The **Application Control** option is enabled by default. Switch the toggle button **Application Control DISABLED** to disable the option.

5. In the **Application Control Settings** block settings, enable the operation mode to apply the Application Control rules and allow Kaspersky Endpoint Security for Windows to block startup of applications.

   If you want to test the Application Control rules, in the **Application Control Settings** section, enable the test mode. In the test mode, Kaspersky Endpoint Security for Windows does not block startup of applications, but logs information about triggered rules in the report. Click the **View report** link to view this information.

6. Enable the **Control DLL modules load** option if you want Kaspersky Endpoint Security for Windows to monitor the loading of DLL modules when applications are started by users.

   Information about the module and the application that loaded the module will be saved to a report.

   Kaspersky Endpoint Security for Windows monitors only the DLL modules and drivers loaded after the **Control DLL modules load** option is selected. Restart the device after selecting the **Control DLL modules load** option if you want Kaspersky Endpoint Security for Windows to monitor all DLL modules and drivers, including those loaded before Kaspersky Endpoint Security for Windows is started.

7. (Optional) In the **Message templates** block, change the template of the message that is displayed when an application is blocked from starting and the template of the email message that is sent to you.

8. In the **Application Control Mode** block settings, select the **Denylist** or **Allowlist** mode.

   By default, the **Denylist** mode is selected.

9. Click the **Rules Lists Settings** link.

   The **Denylists and allowlists** window opens to let you add an application category. By default, the **Denylist** tab is selected if the **Denylist** mode is selected, and the **Allowlist** tab is selected if the **Allowlist** mode is selected.

10. In the **Denylists and allowlists** window, click the **Add** button.

    The **Application Control rule** window opens.

11. Click the **Please choose a category** link.

    The **Application Category** window opens.

12. Add the application category (or categories) that you created earlier.

    You can edit the settings of a created category by clicking the **Edit** button.

    You can create a new category by clicking the **Add** button.

    You can delete a category from the list by clicking the **Delete** button.

13. After the list of application categories is complete, click the **OK** button.

    The **Application Category** window closes.

14. In the **Application Control** rule window, in the **Subjects and their rights** section, create a list of users and groups of users to apply the Application Control rule.

15. Click the **OK** button to save the settings and to close the **Application Control rule** window.

16. Click the **OK** button to save the settings and to close the **Denylists and allowlists** window.

17. Click the **OK** button to save the settings and to close the **Application Control** window.

18. Close the window with the Kaspersky Endpoint Security for Windows policy settings.

Application Control is configured. After the policy is propagated to the client devices, the startup of executable

files is managed.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

# Obtaining and viewing a list of applications installed on client devices

Kaspersky Security Center Linux inventories all software installed on managed client devices running Linux and Windows.

Network Agent compiles a list of applications installed on a device, and then transmits this list to Administration Server. It takes about 10-15 minutes for the Network Agent to update the application list.

For Windows-based client devices, Network Agent receives most of the information about installed applications from the Windows registry. For Linux-based client devices, package managers provide information about installed applications to Network Agent.

*To view the list of applications installed on managed devices:*

1. In the main menu, go to **Software management** → **Third-party applications** → **Applications registry**.

   The page displays a table with the applications that are installed on managed devices. Select the application to view its properties, for example, vendor name, version number, list of executable files, list of devices on which the application is installed.

2. You can group and filter the data of the table with installed applications as follows:

   - Click the settings icon ( ) in the upper-right corner of the table.

     In the invoked **Columns settings** menu, select the columns to be displayed in the table. To view the operating system type of the client devices on which the application is installed, select the **OS type** column.

   - Click the filter icon ( ) in the upper-right corner of the table, and then specify and apply the filter criterion in the invoked menu.

     The filtered table of installed applications is displayed.

*To view the list of applications installed on a specific managed device,*

In the main menu, go to **Asset management** → **Managed devices** → **<device name>** → **Advanced** → **Applications registry**. In this menu, you can export the list of applications to a CSV file or TXT file.

For detailed information about Application Control, refer to the Kaspersky Endpoint Security for Linux Help and Kaspersky Endpoint Security for Windows Help.

# About third-party applications

Kaspersky Security Center Linux can help you to update third-party software, installed on client devices, and fix the vulnerabilities of the third-party software. Kaspersky Security Center Linux can update third-party software from the current version to the latest version only.

> The list of third-party software can be changed and it is updated dynamically. You can check whether you can update the third-party software (installed on users' devices) with Kaspersky Security Center Linux by viewing the list of available updates in Kaspersky Security Center Web Console.

The procedure outlined below is intended solely for viewing the list of third-party software that can be updated with Kaspersky Security Center Linux. The steps are followed to access the relevant information without initiating any tasks.

*To view the list of third-party software that you can update with Kaspersky Security Center Linux:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.
3. At the **New task settings** step of the wizard, specify the following settings:
   a. In the **Application** drop-down list, select **Kaspersky Security Center Linux**.
   b. In the **Task type** field, select **Install required updates and fix vulnerabilities**.
4. At the **Task scope** step of the wizard, select the **Managed Devices** option.
5. At the **Specify rules for installing updates** step of the wizard, click the **Add** button.

   The Rule creation wizard starts. Proceed through the wizard by using the **Next** button.
6. At the **Select rule type** step of the wizard, select the **Rule for third-party updates** option.
7. At the **General criteria** step of the wizard, select the **Install all updates (except declined)** option, and then click **Next**.

The list of third-party software is displayed.

# Installing third-party software updates

Kaspersky Security Center Linux allows you to manage the updates of third-party software installed on managed devices and fix vulnerabilities in such software through the installation of required updates.

Kaspersky Security Center Linux searches for updates through the *Find vulnerabilities and required updates* task. When this task is complete, Administration Server receives the lists of detected vulnerabilities and required updates for the third-party software installed on the devices that you specified in the task properties. After viewing information about available updates, you can install them on your devices.

Kaspersky Security Center Linux updates some applications by removing the previous version of the application and installing the new one.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it is currently open.

For security reasons, any third-party software updates that you install by using the Vulnerability and patch management feature are automatically scanned for malware by Kaspersky technologies. These technologies are used for automatic file checks and include virus scanning, static analysis, dynamic analysis, behavior analysis in the sandbox environment, and machine learning.

Kaspersky experts do not perform manual analysis of third-party software updates that can be installed by using the Vulnerability and patch management feature. In addition, Kaspersky experts do not search for vulnerabilities (known or unknown) or undocumented features in such updates, nor do they perform other types of analysis of the updates other than those specified in the paragraph above.

When the metadata of third-party software updates is downloaded to the repository, you can install the updates on client devices by using the *Install required updates and fix vulnerabilities* task.

> The *Install required updates and fix vulnerabilities* task can be created only if you have the license for the Vulnerability and patch management feature.

When this task is complete, the updates are installed on the managed devices automatically. When the metadata of new updates is downloaded to the Administration Server repository, Kaspersky Security Center Linux checks whether the updates meet the criteria specified in the update rules. All new updates that meet the criteria will be downloaded and installed automatically at the next task run.

# Scenario: Updating third-party software

This section provides a scenario for updating third-party software installed on client devices. Third-party software includes applications from other software vendors.

## Prerequisites

The Administration Server must be connected to the internet in order to install third-party software updates.

## Stages

Updating third-party software proceeds in stages:

1. **Searching for required updates**

   To find the third-party software updates required for the managed devices, run the *Find vulnerabilities and required updates* task. When this task is complete, Kaspersky Security Center Linux receives the lists of detected vulnerabilities and required updates for the third-party software installed on the devices that you specified in the task properties.

The *Find vulnerabilities and required updates* task is created automatically by the Administration Server quick start wizard. If you did not run the wizard, create the *Find vulnerabilities and required updates* task or run the quick start wizard now.

> You can create the *Find vulnerabilities and required updates* task only for Windows devices. You cannot create this task for devices running on other operating systems.

2. **Viewing the list of found updates**

View information about the available third-party software updates and decide which updates you want to install. To view detailed information about each update, click the update name in the list. For each update in the list, you can also view the statistics on the update installation on client devices.

3. **Configuring installation of updates**

When Kaspersky Security Center Linux receives the list of third-party software updates, you can install them on client devices by creating the *Install required updates and fix vulnerabilities* task.

> You can create the *Install required updates and fix vulnerabilities* task only for Windows devices. You cannot create this task for devices running on other operating systems.

The *Install required updates and fix vulnerabilities* task is used to install updates for Microsoft applications, including the updates provided by the Windows Update service, and updates of other vendors' software. Note that the *Install required updates and fix vulnerabilities* task can be created only if you have a license for the Vulnerability and patch management feature.

To install some software updates you must accept the End User License Agreement (EULA) for the installation software. If you decline the EULA, the software update will not be installed.

You can start an update installation task by schedule. When specifying the task schedule, make sure that the update installation task starts after the *Find vulnerabilities and required updates* task is complete.

4. **Scheduling the tasks**

To be sure that the update list is always up-to-date, schedule the *Find vulnerabilities and required updates* task to run the task automatically from time to time. By default, the *Find vulnerabilities and required updates* task is set to start manually.

If you have created the *Install required updates and fix vulnerabilities* task, you can schedule it to run with the same frequency as the *Find vulnerabilities and required updates* task or less often.

When scheduling the tasks, make sure that an update installation task starts after the *Find vulnerabilities and required updates* task is complete.

5. **Approving and declining third-party software updates (optional)**

If you have created the *Install required updates and fix vulnerabilities* task, you can specify rules for the update installation in the task properties window.

For each rule, you can define the updates to install depending on the update status: *Undefined*, *Approved*, or *Declined*. For example, you may want to create a specific task for servers and set a rule for this task to allow installation of only those updates that have the *Approved* status. After that, you manually set the *Approved* status for those updates that you want to install. In this case, the updates that have the *Undefined* or *Declined* status will not be installed on the servers that you specified in the task.

The usage of the *Approved* status to manage update installation is efficient for a small amount of updates. To install multiple updates, use the rules that you can configure in the *Install required updates and fix vulnerabilities* task. We recommend that you set the *Approved* status for only those specific updates that do not meet the criteria specified in the rules. If you manually approve a large number of updates, the performance of the Administration Server decreases, which may lead to an overload of the Administration Server.

By default, downloaded software updates have the *Undefined* status. You can change the status to *Approved* or *Declined* in the **Software updates** list (**Software management** → **Patch management** → **Software updates**).

For more details, refer to the instructions on approving and declining third-party software updates.

6. **Running an update installation task**

   Start the *Install required updates and fix vulnerabilities* task. When you start this task, updates are downloaded and installed on managed devices. After the task is complete, make sure that it has the *Completed successfully* status in the task list.

7. **Create a report on the results of the update installation (optional)**

   To view detailed statistics on the update installation, create the Report on results of installation of third-party software updates.

Results

If you have created and configured the *Install required updates and fix vulnerabilities* task, the updates are installed on the managed devices automatically. When new updates are downloaded to the Administration Server repository, Kaspersky Security Center Linux checks whether they meet the criteria specified in the update rules. All new updates that meet the criteria will be installed automatically at the next task run.

# Third-party software updates installation options

You can install third-party software updates and updates from Windows Update on managed devices by creating and running the *Install required updates and fix vulnerabilities* task. The *Install required updates and fix vulnerabilities* task can be created only if you have a license for the Vulnerability and patch management feature. You can use this task to install the updates of other vendors' software.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it is currently open.

As an option, you can create a task to install the required updates in the following ways:

- By opening the update list, and then specifying which updates to install.

  As a result, a new task to install the selected updates is created. As an option, you can add the selected updates to an existing task.

- By running the Update installation wizard.

  The Update installation wizard is only available under the Vulnerability and patch management license.

  The wizard simplifies creation and configuration of an update installation task, and enables you to eliminate the creation of redundant tasks that contain the same updates to install.

### Installing third-party software updates by using the update list

*To install third-party software updates by using the list of updates:*

1. Open the list of updates by using one of the following paths:

   - **Software management** → **Patch management** → **Software updates**.
   - **Asset management** → **Managed devices** → <device name> → **Advanced** → **Available updates**.
   - **Software management** → **Third-party applications** → **Applications registry** → <application name> → **Available updates**.

   A list of available updates appears.

2. Select the check boxes next to the updates that you want to install.

3. Click the **Install updates** button. If this button is not visible, click the ellipsis button, and then select **Install updates** from the drop-down list.

   To install some software updates, you must accept the End User License Agreement (EULA). If you decline the EULA, the software update is not installed.

4. Choose one of the following options:

   - **New task**

     The New task wizard starts. If you have the Vulnerability and patch management license, the *Install required updates and fix vulnerabilities* task is preselected. Follow the steps of the wizard to complete the task creation.

   - **Install update (add rule to specified task)**

     Select a task to which you want to add the selected updates. If you have the Vulnerability and patch management license, select the *Install required updates and fix vulnerabilities* task. A new rule to install the selected updates is automatically added to the selected task. The selected updates are added to the task properties.

     The task properties window opens. Click **Save** to save the changes.

   If you have chosen to create a task, the task is created and displayed in the task list at **Tasks**. If you have chosen to add the updates to an existing task, the updates are saved in the task properties.

To install third-party software updates, you have to start the *Install required updates and fix vulnerabilities* task. You can start this task by clicking the **Start** button in the task list or by specifying schedule settings in the properties of the task that you start. When specifying the task schedule, make sure that the update installation task starts after the *Find vulnerabilities and required updates* task is complete.

### Installing third-party software updates by using the Update installation wizard

The Update installation wizard is only available under the Vulnerability and patch management license.

*To create a task to install third-party software updates by using the Update installation wizard:*

1. In the main menu, go to **Software management → Patch management → Software updates**.

   A list of available updates appears.

2. Select the check box next to the update that you want to install.

3. Click the **Run Update installation wizard** button.

   The Update installation wizard starts. The **Select the update installation task** page displays the list of all existing tasks of the following types:

   - *Install required updates and fix vulnerabilities*
   - *Fix vulnerabilities*

4. If you want the wizard to display only those tasks that install the update that you selected, then enable the **Show only tasks that install this update** option.

5. Choose what you want to do:

   - To start an existing task, select the check box next to the *Install required updates and fix vulnerabilities* task, and then click the **Start** button.

     The task will complete in background mode. No further actions are required.

   - To add a new rule to an existing task:

     a. Select the check box next to the task name, and then click the **Add rule** button.

     > The **Add rule** button is disabled if you select more than one task.

     You cannot add a rule for a *Fix vulnerabilities* task. If you select a *Fix vulnerabilities* task, the following notification appears: "*To install updates, use the "Install required updates and fix vulnerabilities" task.*"

     b. At the **Create update installation rule** step of the wizard, configure the new rule:

     - **Installation rule for updates of this importance level**

       Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

       If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the severity of the selected update (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

       If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

       By default, this option is disabled.

       This rule is not displayed if the importance level of the selected update is *Unknown*.

     - **Installation rule for updates of this importance level according to MSRC**

       Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled (available only for Windows Update updates), the updates fix only those vulnerabilities for which the severity level set by Microsoft Security Response Center (MSRC) is equal to or higher than the value selected in the list (**Low**, **Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

This rule is displayed only for Microsoft software updates. It is not displayed if the importance level of the selected update is *Unknown*.

- **Installation rule for updates by this vendor**

  This option is available only for updates of third-party applications. Kaspersky Security Center Linux installs only those updates that relate to the applications made by the same vendor as the selected update. Declined updates and updates to the applications made by other vendors are not installed.

  By default, this option is disabled.

  This rule is displayed only for third-party software updates.

- **Installation rule for updates of the type**

- **Installation rule for updates of the selected application**

  This rule is displayed only for third-party software updates.

- **Installation rule for the selected update**

- **Approve selected updates**

  The selected update will be approved for installation. Enable this option if some applied rules of update installation allow installation of approved updates only.

  By default, this option is disabled.

- **Automatically install all previous application updates that are required to install the selected updates**

  Keep this option enabled if you agree with the installation of interim application versions when this is required for installing the selected updates.

  If this option is disabled, only the selected versions of applications are installed. Disable this option if you want to update applications in a straightforward manner, without attempting to install successive versions incrementally. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

  For example, you have version 3 of an application installed on a device and you want to update it to version 5, but version 5 of this application can be installed only over version 4. If this option is enabled, the software first installs version 4, and then installs version 5. If this option is disabled, the software fails to update the application.

  By default, this option is enabled.

c. Click **Add**.

The task properties window opens. The new rule is already added to the task properties. You can view or modify the rule, or other task settings. Click **Save** to save the changes.

- To create a task:

  a. Click the **New task** button.

  b. At the **Create update installation rule** step of the wizard, configure the new rule:

  - **Installation rule for updates of this importance level**

    Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

    If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the severity of the selected update (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

    If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

    By default, this option is disabled.

    This rule is not displayed if the importance level of the selected update is *Unknown*.

  - **Installation rule for updates of this importance level according to MSRC**

    Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

    If this option is enabled (available only for Windows Update updates), the updates fix only those vulnerabilities for which the severity level set by Microsoft Security Response Center (MSRC) is equal to or higher than the value selected in the list (**Low**, **Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

    If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

    By default, this option is disabled.

    This rule is displayed only for Microsoft software updates. It is not displayed if the importance level of the selected update is *Unknown*.

  - **Installation rule for updates by this vendor**

    This option is available only for updates of third-party applications. Kaspersky Security Center Linux installs only those updates that relate to the applications made by the same vendor as the selected update. Declined updates and updates to the applications made by other vendors are not installed.

    By default, this option is disabled.

    This rule is displayed only for third-party software updates.

  - **Installation rule for updates of the type**

  - **Installation rule for updates of the selected application**

    This rule is displayed only for third-party software updates.

  - **Installation rule for the selected update**

  - **Approve selected updates**

    The selected update will be approved for installation. Enable this option if some applied rules of update installation allow installation of approved updates only.

By default, this option is disabled.

- **Automatically install all previous application updates that are required to install the selected updates**

  Keep this option enabled if you agree with the installation of interim application versions when this is required for installing the selected updates.

  If this option is disabled, only the selected versions of applications are installed. Disable this option if you want to update applications in a straightforward manner, without attempting to install successive versions incrementally. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

  For example, you have version 3 of an application installed on a device and you want to update it to version 5, but version 5 of this application can be installed only over version 4. If this option is enabled, the software first installs version 4, and then installs version 5. If this option is disabled, the software fails to update the application.

  By default, this option is enabled.

c. Click **Add**.

Continue to create the task in the New task wizard. The new rule that you added in the Update installation wizard is displayed in the New task wizard. When you complete the wizard, the *Install required updates and fix vulnerabilities* task is added to the task list.

# Find vulnerabilities and required updates task settings

The *Find vulnerabilities and required updates* task is created automatically when the quick start wizard is running. If you did not run the wizard, you can create the task manually.

In addition to the general task settings, you can specify the following settings when creating the *Find vulnerabilities and required updates* task or later, when configuring the properties of the created task:

- **Search for vulnerabilities and updates listed by Microsoft**

  When searching for vulnerabilities and updates, Kaspersky Security Center Linux uses the information about applicable Microsoft updates from the source of Microsoft updates, which are available at the present moment.

  For example, you may want to disable this option if you have different tasks with different settings for Microsoft updates and updates of third-party applications.

  By default, the option is enabled.

  Information about optional Microsoft Windows updates is not being sent to the Administration Server.

- **Connect to the update server to update data**

  Windows Update Agent on a managed device connects to the source of Microsoft updates. The following servers can act as a source of Microsoft updates:

  - Windows Server with Microsoft Windows Server Update Services (WSUS) deployed in your organization's network
  - Microsoft Updates servers

  If this option is enabled, Windows Update Agent on a managed device connects to the source of Microsoft updates to refresh the information about applicable Microsoft Windows updates.

If this option is disabled, Windows Update Agent on a managed device uses the information about applicable Microsoft Windows updates that was received from the source of Microsoft updates earlier.

Connecting to the source of Microsoft updates can be resource-consuming. You might want to disable this option if you set regular connection to this source of updates in another task or in the properties of Network Agent policy, in the section **Software updates and vulnerabilities**. If you do not want to disable this option, then, to reduce the Server overload, you can configure the task schedule to randomize delay for task starts within 360 minutes.

By default, the option is enabled.

Combination of the following options of the settings of Network Agent policy defines the mode of getting updates:

- The Windows Update Agent on a managed device connects to the update server to receive updates only if the **Connect to the update server to update data** setting is enabled in the properties of the *Find vulnerabilities and required updates* task and the **Windows Update search mode** is set to **Active** in the Network Agent policy settings.

- If you do not need Network Agent to initiate a connection to the Microsoft Windows update source and download updates when performing the *Vulnerability scan* task, you can set the **Windows Update search mode** option to **Passive**, while the **Connect to the update server to update data** option must remain enabled. This allows for you to save resources and use previously received Windows updates to scan for vulnerabilities. You can use the passive mode if you configure receiving Microsoft Windows updates in a different way. If receiving Microsoft Windows updates is not configured in another way, do not set the **Windows Update search mode** option to **Passive**, because in this case, information about updates will never be received.

- Irrespective of the **Connect to the update server to update data** option's status (enabled or disabled), if the **Windows Update search mode** option is set to **Disabled**, Kaspersky Security Center Linux does not request any information about updates.

If in the network of your organization the WSUS server is used (local WSUS server), and you want to use it together with Kaspersky Security Center Administration Server, you must first ensure that Kaspersky Security Center Administration Server is not used as a WSUS server, and then do the following:

1. On your managed devices running Windows, specify your local WSUS server for the Windows Update service. You can do it either manually in Windows Registry or by using a Windows group policy.

2. On your local WSUS server, specify the required classifications for updates and the applications on which the updates are to be distributed.

3. Synchronize your WSUS server with the upstream server (this can be either a Microsoft WSUS server or another local upstream WSUS server).

After the *Find vulnerabilities and required updates* task is run on the device, Network Agent uses the Windows Update service to initiate a request for Windows updates applicable to the device. The Windows Update service obtains the address of the external WSUS server from the registry and searches for updates directly from that external WSUS server. Then, the Windows Update service forwards this list to the Administration Server through Network Agent. Thus, Administration Server has an up-to-date base.

- **Search for third-party vulnerabilities and updates listed by Kaspersky**

  If this option is enabled, Kaspersky Security Center Linux searches for vulnerabilities and required updates for third-party applications (applications made by software vendors other than Kaspersky and Microsoft) in Windows Registry and in the folders specified under **Specify paths for advanced search of applications in file system**. The full list of supported third-party applications is managed by Kaspersky.

If this option is disabled, Kaspersky Security Center Linux does not search for vulnerabilities and required updates for third-party applications. For example, you may want to disable this option if you have different tasks with different settings for Microsoft Windows updates and updates of third-party applications.

By default, the option is enabled.

- **Specify paths for advanced search of applications across the file system**

  The folders in which Kaspersky Security Center Linux searches for third-party applications that require vulnerability fix and update installation. You can use system variables.

  Specify the folders to which applications are installed. By default, the list contains system folders to which most of the applications are installed.

- **Enable advanced diagnostics**

  If this feature is enabled, Network Agent writes trace files even if writing trace files is disabled for Network Agent in Kaspersky Security Center Linux Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size, in MB, of advanced diagnostics files** value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility, you can download or delete them there.

  If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Linux Remote Diagnostics Utility. No additional traces are written.

  When creating a task, you do not have to enable advanced diagnostics. You may want to use this feature later if, for example, a task run fails on some of the devices and you want to get additional information during another task run.

  By default, this option is disabled.

- **Maximum size, in MB, of advanced diagnostics files**

  The default value is 100 MB, and available values are between 1 MB and 2048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

## Recommendations on the task schedule

When scheduling the *Find vulnerabilities and required updates* task, make sure that two options—**Run missed tasks** and **Use automatically randomized delay for task starts**—are enabled.

By default, the *Find vulnerabilities and required updates* task is set to start manually. If the organization's workplace rules provide for shutting down all devices at this time, the *Find vulnerabilities and required updates* task will run after the devices are turned on again, that is, the following morning. Such activity may be undesirable because a vulnerability scan may increase the load on CPUs and disk subsystems. You must set up the most convenient schedule for the task based on the workplace rules adopted in the organization.

# Creating the Find vulnerabilities and required updates task

Through the *Find vulnerabilities and required updates* task, Kaspersky Security Center Linux receives lists of detected vulnerabilities and required updates for the third-party software installed on the managed devices.

You can create the *Find vulnerabilities and required updates* task only for Windows devices. You cannot create this task for devices running on other operating systems.

The *Find vulnerabilities and required updates* task is created automatically when the quick start wizard is running. If you did not run the wizard, you can create the task manually.

*To create the Find vulnerabilities and required updates task:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.
3. For the Kaspersky Security Center application, select the **Find vulnerabilities and required updates** task type.
4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).
5. Select the devices to which the task will be assigned.
6. Specify the methods to scan for vulnerabilities and applications that require updating:

   - **Search for vulnerabilities and updates listed by Microsoft**

     When searching for vulnerabilities and updates, Kaspersky Security Center Linux uses the information about applicable Microsoft updates from the source of Microsoft updates, which are available at the present moment.

     For example, you may want to disable this option if you have different tasks with different settings for Microsoft updates and updates of third-party applications.

     By default, the option is enabled.

     Information about optional Microsoft Windows updates is not being sent to the Administration Server.

     - **Connect to the update server to update data**

       Windows Update Agent on a managed device connects to the source of Microsoft updates. The following servers can act as a source of Microsoft updates:

       - Windows Server with Microsoft Windows Server Update Services (WSUS) deployed in your organization's network
       - Microsoft Updates servers

       If this option is enabled, Windows Update Agent on a managed device connects to the source of Microsoft updates to refresh the information about applicable Microsoft Windows updates.

If this option is disabled, Windows Update Agent on a managed device uses the information about applicable Microsoft Windows updates that was received from the source of Microsoft updates earlier.

Connecting to the source of Microsoft updates can be resource-consuming. You might want to disable this option if you set regular connection to this source of updates in another task or in the properties of Network Agent policy, in the section **Software updates and vulnerabilities**. If you do not want to disable this option, then, to reduce the Server overload, you can configure the task schedule to randomize delay for task starts within 360 minutes.

By default, the option is enabled.

Combination of the following options of the settings of Network Agent policy defines the mode of getting updates:

- The Windows Update Agent on a managed device connects to the update server to receive updates only if the **Connect to the update server to update data** setting is enabled in the properties of the *Find vulnerabilities and required updates* task and the **Windows Update search mode** is set to **Active** in the Network Agent policy settings.

- If you do not need Network Agent to initiate a connection to the Microsoft Windows update source and download updates when performing the *Vulnerability scan* task, you can set the **Windows Update search mode** option to **Passive**, while the **Connect to the update server to update data** option must remain enabled. This allows for you to save resources and use previously received Windows updates to scan for vulnerabilities. You can use the passive mode if you configure receiving Microsoft Windows updates in a different way. If receiving Microsoft Windows updates is not configured in another way, do not set the **Windows Update search mode** option to **Passive**, because in this case, information about updates will never be received.

- Irrespective of the **Connect to the update server to update data** option's status (enabled or disabled), if the **Windows Update search mode** option is set to **Disabled**, Kaspersky Security Center Linux does not request any information about updates.

If in the network of your organization the WSUS server is used (local WSUS server), and you want to use it together with Kaspersky Security Center Administration Server, you must first ensure that Kaspersky Security Center Administration Server is not used as a WSUS server, and then do the following:

1. On your managed devices running Windows, specify your local WSUS server for the Windows Update service. You can do it either manually in Windows Registry or by using a Windows group policy.

2. On your local WSUS server, specify the required classifications for updates and the applications on which the updates are to be distributed.

3. Synchronize your WSUS server with the upstream server (this can be either a Microsoft WSUS server or another local upstream WSUS server).

After the *Find vulnerabilities and required updates* task is run on the device, Network Agent uses the Windows Update service to initiate a request for Windows updates applicable to the device. The Windows Update service obtains the address of the external WSUS server from the registry and searches for updates directly from that external WSUS server. Then, the Windows Update service forwards this list to the Administration Server through Network Agent. Thus, Administration Server has an up-to-date base.

- **Search for third-party vulnerabilities and updates listed by Kaspersky**

  If this option is enabled, Kaspersky Security Center Linux searches for vulnerabilities and required updates for third-party applications (applications made by software vendors other than Kaspersky and Microsoft) in Windows Registry and in the folders specified under **Specify paths for advanced search of applications in file system**. The full list of supported third-party applications is managed by Kaspersky.

  If this option is disabled, Kaspersky Security Center Linux does not search for vulnerabilities and required updates for third-party applications. For example, you may want to disable this option if you have different tasks with different settings for Microsoft Windows updates and updates of third-party applications.

  By default, the option is enabled.

You can disable these options after task creation on the **Application settings** tab of the task properties window.

7. **Specify paths for advanced search of applications across the file system**

   The folders in which Kaspersky Security Center Linux searches for third-party applications that require vulnerability fix and update installation. You can use system variables.

   Specify the folders to which applications are installed. By default, the list contains system folders to which most of the applications are installed.

   You can change the specified paths after task creation on the **Application settings** tab of the task properties window.

8. If required, **Enable advanced diagnostics**

   If this feature is enabled, Network Agent writes trace files even if writing trace files is disabled for Network Agent in Kaspersky Security Center Linux Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size, in MB, of advanced diagnostics files** value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility, you can download or delete them there.

   If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Linux Remote Diagnostics Utility. No additional traces are written.

   When creating a task, you do not have to enable advanced diagnostics. You may want to use this feature later if, for example, a task run fails on some of the devices and you want to get additional information during another task run.

   By default, this option is disabled.

   You can disable this option after task creation on the **Application settings** tab of the task properties window.

9. Specify the **Maximum size, in MB, of advanced diagnostics files**

   The default value is 100 MB, and available values are between 1 MB and 2048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

   You have to specify this value if you enabled advanced diagnostics in the previous step. You can change this value after task creation on the **Application settings** tab of the task properties window.

10. If you want to modify the default task settings, enable the **Open task details when creation is complete** option on the **Finish task creation** page. If you do not enable this option, the task is created with the default settings. You can change the default settings later, at any time.

11. Click the **Finish** button.

The wizard creates the task. If you enabled the **Open task details when creation is complete** option, the task properties window automatically opens. In this window, you can specify the general task settings and, if required, change the settings specified during task creation.

> You can also open the task properties window by clicking the name of the created task in the list of tasks.

The task is created and configured. To run the task, select it in the task list, and then click the **Start** button.

Recommendations on the task schedule

When scheduling the *Find vulnerabilities and required updates* task, make sure that two options—**Run missed tasks** and **Use automatically randomized delay for task starts**—are enabled.

By default, the *Find vulnerabilities and required updates* task is set to start manually.

You can also schedule the *Find vulnerabilities and required updates* task to start at a particular time. For example, you can select the **Every N hours** scheduled start from the **Start task** drop-down list on the **Schedule** tab of the task properties window. In this case, note that if the organization's workplace rules provide for shutting down all devices at this time, the *Find vulnerabilities and required updates* task will run after the devices are turned on again. Such activity may be undesirable because a vulnerability scan may increase the load on CPUs and disk subsystems. You must set up the most convenient schedule for the task based on the workplace rules adopted in the organization.

For a detailed description of scheduled start settings, refer to the general task settings.

# Viewing information about available third-party software updates

You can view the list of available updates for third-party software, including Microsoft software, installed on client devices.

*To view the list of available updates for third-party applications installed on client devices,*

In the main menu, go to **Software management** → **Patch management** → **Software updates**.

A list of available updates appears.

You can specify a filter to view the list of software updates. Click the **Filter** icon ( ) of the software updates list to manage the filter. You can also select one of the preset filters from the **Preset filters** drop-down list above the software vulnerabilities list.

*To view the properties of an update:*

1. Click the name of the required software update.
2. The properties window of the update opens, displaying information grouped on the following tabs:

- **General**

  This tab displays general details of the selected update:

  - Update approval status (can be changed manually by selecting a new status in the drop-down list)
  - Date and time the update was registered
  - Date and time the update was created
  - Importance level of the update
  - Installation requirements imposed by the update
  - Application family to which the update belong
  - Application to which the update applies
  - Number of the update revision

- **Attributes**

  This tab displays a set of attributes that you can use to obtain more information about the selected update. This set differs depending on whether the update is published by Microsoft or by a third-party vendor.

  The tab displays the following information for a Microsoft update:

  - Importance level of the update according to the Microsoft Security Response Center (MSRC)
  - Link to the article in the Microsoft Knowledge Base describing the update
  - Link to the article in the Microsoft Security Bulletin describing the update
  - Update identifier (ID)

  The tab displays the following information for a third-party update:

  - Whether the update is a patch or a full distribution package
  - Localization language of the update
  - Whether the update is installed automatically or manually
  - Whether the update was revoked after being applied
  - Link for downloading the update

- **Devices**

  This tab displays a list of devices on which the selected update has been installed.

- **Fixed vulnerabilities**

  This tab displays a list of vulnerabilities that the selected update can fix.

- **Crossover of updates**

  This tab displays possible crossovers between various updates published for the same application, that is, whether the selected update can supersede other updates or, vice versa, be superseded by other updates (available for Microsoft updates only).

- **Tasks to install this update**

  This tab displays a list of tasks whose scope includes installation of the selected update. The tab also enables you to create a new remote installation task for the update.

*To view the statistics of an update installation:*

1. Select the check box next to the required software update.

2. Click the **Statistics of update installation statuses** button.

The diagram of the update installation statuses is displayed. Clicking a status opens a list of devices that have the selected status.

You can view information about available software updates for third-party software, including Microsoft software, installed on the selected managed device running Windows.

*To view the list of available updates for third-party software installed on the selected managed device:*

1. In the main menu, go to **Asset management** → **Managed devices**.

   The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the device for which you want to view third-party software updates.

   The properties window of the selected device is displayed.

3. In the properties window of the selected device, select the **Advanced** tab.

4. In the left pane, select the **Available updates** section. If you want to view only installed updates, enable the **Show installed updates** option.

The list of available third-party software updates for the selected device is displayed.

# Exporting the list of available software updates to a file

You can export the list of updates for third-party software, including Microsoft software, to a CSV or TXT file. You can use these files, for example, to send to your information security manager or to store them for statistical purposes.

*To export to a text file the list of available updates for third-party software installed on all managed devices:*

1. In the main menu, go to **Operations** → **Patch management** → **Software updates**.

   A list of available updates appears.

If you want to export a complete list of software updates, only updates displayed on the current page will be exported.

If you want to export only particular updates, select the check boxes next to the required updates in the list.

2. Click the **Export to TXT** or **Export to CSV** button, depending on the format you prefer. If either of these buttons is not visible, click the ellipsis button, and then select the required option from the drop-down list.

The file containing the list of available updates for third-party software, including Microsoft software, is downloaded to your current device.

*To export to a text file the list of available updates for third-party software installed on the selected managed device:*

1. Open the list of available third-party software updates on the selected managed device.

   A list of available updates appears.

   If you want to export a complete list of software updates, only updates displayed on the current page will be exported.

   If you want to export only particular updates, select the check boxes next to the required updates in the list.

   If you want to export only installed updates, select the **Show installed updates** check box.

2. Click the **Export to TXT** or **Export to CSV** button, depending on the format you prefer. If either of these buttons is not visible, click the ellipsis button, and then select the required option from the drop-down list.

The file containing the list of available updates for third-party software, including Microsoft software, installed on the selected managed device is downloaded to your current device.

# Approving and declining third-party software updates

When you configure the *Install required updates and fix vulnerabilities* task, you can create a rule that requires a specific status of updates that are to be installed. For example, an update rule can allow installation of the following:

- Only approved updates
- Only approved and undefined updates
- All updates irrespective of the update statuses

You can approve updates that must be installed and decline updates that must not be installed.

The usage of the *Approved* status to manage update installation is efficient for a small amount of updates. To install multiple updates, use the rules that you can configure in the properties of the *Install required updates and fix vulnerabilities* task. We recommend that you set the *Approved* status for only those specific updates that do not meet the criteria specified in the rules. When you manually approve a large number of updates, the performance of the Administration Server decreases, which may lead to an overload of the Administration Server.

*To approve or decline one or several updates:*

1. In the main menu, go to **Software management** → **Patch management** → **Software updates**.

   A list of available updates appears.

2. Select the updates that you want to approve or decline.

3. Click the **Approve** button to approve the selected updates or the **Decline** button to decline the selected updates. If either of these buttons is not visible, click the ellipsis button, and then select the required option from the drop-down list.

   The default status of an update is *Undefined*.

The selected updates have the statuses that you defined.

As an option, you can change the approval status in the properties of a specific update.

*To approve or decline an update in its properties:*

1. In the main menu, go to **Software management** → **Patch management** → **Software updates**.

   A list of available updates appears.

2. Click the name of the update that you want to approve or decline.

   The update properties window opens.

3. In the **General** section, select a status for the update in the **Update approval status** drop-down list. You can select the *Approved*, *Declined*, or *Undefined* status.

4. Click **Save** to save the changes.

The selected update has the status that you defined.

If you set the *Declined* status for third-party software updates, these updates will not be installed on devices for which they were planned but have not yet been installed. Updates will remain on devices on which they were already installed. If necessary, you can manually delete them locally.

# Creating the Install required updates and fix vulnerabilities task

The *Install required updates and fix vulnerabilities* task is only available under the Vulnerability and patch management license.

The *Install required updates and fix vulnerabilities* task is used to update and fix vulnerabilities in the third-party software installed on managed devices. This task allows you to install multiple updates and fix multiple vulnerabilities according to the rules, which you specify in the task settings.

To install updates or fix vulnerabilities by using the *Install required updates and fix vulnerabilities* task, you can do one of the following:

- Run the Update installation wizard or the Vulnerability fix wizard.
- Create an *Install required updates and fix vulnerabilities* task.
- Add a rule for update installation to an existing *Install required updates and fix vulnerabilities* task.

*To create the Install required updates and fix vulnerabilities task:*

1. In the main menu, go to **Tasks**.
2. Click **Add**.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.
3. In the **Application** drop-down list, select Kaspersky Security Center Linux.
4. In the **Task type** list, select the **Install required updates and fix vulnerabilities** task type.

   If the task is not displayed, make sure that your account has the **Read**, **Write**, and **Execute** rights for the **System management**: **Vulnerability and patch management** functional area. You cannot create and configure the *Install required updates and fix vulnerabilities* task without these access rights.
5. In the **Task name** field, specify the name of the new task.

   The task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).
6. Select devices to which the task will be assigned.
7. Add the update installation rules at the **Specify rules for installing updates** step of the wizard.

   These rules are applied to installation of updates on client devices. If rules are not specified, the task has nothing to perform. For information about operations with rules, refer to Rules for update installation.

   These rules are applied to the installation of updates on client devices. If you do not specify any rules, the task has nothing to perform.
8. Specify the following parameters:

   - **Start installation at device restart or shutdown**

     If this option is enabled, updates are installed when the device is restarted or shut down. Otherwise, updates are installed according to a schedule.

     Use this option if installing the updates might affect the device performance.

     By default, this option is disabled.

   - **Install the required general system components**

     If this option is enabled, before installing an update the application automatically installs all general system components (prerequisites) that are required to install the update. For example, these prerequisites can be operating system updates.

     If this option is disabled, you may have to install the prerequisites manually.

     By default, this option is disabled.

   - **Allow installation of new application versions during updates**

     If this option is enabled, updates are allowed when they result in installation of a new version of a software application.

     If this option is disabled, the software is not upgraded. You can then install new versions of the software manually or through another task. For example, you may use this option if your company infrastructure is not supported by a new software version or if you want to check an upgrade in a test infrastructure.

By default, the option is enabled.

> Upgrading an application may cause malfunction of dependent applications installed on client devices.

- **Download updates to the device without installing them**

  If this option is enabled, the application downloads updates to the device but does not install them automatically. You can then Install downloaded updates manually.

  Microsoft updates are downloaded to the system Windows storage. Updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft) are downloaded to the folder specified in the **Download updates to** field.

  If this option is disabled, the updates are installed to the device automatically.

  By default, this option is disabled.

  - **Download updates to**

    This folder is used to download updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft).

- **Enable advanced diagnostics**

  If this feature is enabled, Network Agent writes trace files even if writing trace files is disabled for Network Agent in Kaspersky Security Center Linux Remote Diagnostics Utility. Traces are written to two files in turn; the total size of both files is determined by the **Maximum size, in MB, of advanced diagnostics files** value. When both files are full, Network Agent starts writing to them again. The files with traces are stored in the %WINDIR%\Temp folder. These files are accessible in the remote diagnostics utility, you can download or delete them there.

  If this feature is disabled, Network Agent writes traces according to the settings in Kaspersky Security Center Linux Remote Diagnostics Utility. No additional traces are written.

  When creating a task, you do not have to enable advanced diagnostics. You may want to use this feature later if, for example, a task run fails on some of the devices and you want to get additional information during another task run.

  By default, this option is disabled.

  - **Maximum size, in MB, of advanced diagnostics files**

    The default value is 100 MB, and available values are between 1 MB and 2048 MB. You may be asked to change the default value by Kaspersky Technical Support specialists when information in the advanced diagnostics files sent by you is not enough to troubleshoot the problem.

Go to the next step of the wizard.

9. Specify the operating system restart settings:

- **Do not restart the device**

  Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- **Restart the device**

  Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action**

  The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

  By default, this option is selected.

- **Repeat prompt every (min)**

  If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

  By default, the option is enabled. The default interval is 5 minutes. Available values are between 1 and 1440 minutes.

  If this option is disabled, the prompt is displayed only once.

- **Restart after (min)**

  After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

  By default, the option is enabled. The default delay is 30 minutes. Available values are between 1 and 1440 minutes.

- **Wait time before forced closure of applications in blocked sessions (min)**

  Applications are forced to close when the user's device goes locked (automatically after a specified interval of inactivity, or manually).

  If this option is enabled, applications are forced to close on the locked device upon expiration of the time interval specified in the entry field.

  If this option is disabled, applications do not close on the locked device.

  By default, this option is disabled.

10. At the **Finish task creation** step of the wizard, enable the **Open task details when creation is complete** option to modify the default task settings.

    If you do not enable this option, the task is created with the default settings. You can modify the default settings later.

11. Click the **Finish** button.

    The New task wizard creates the task. If you enabled the **Open task details when creation is complete** option, the task properties window automatically opens. In this window, you can specify the general task settings and, if required, change the settings specified during task creation.

    > You can also open the task properties window by clicking the name of the created task in the list of tasks.

    The task is created, configured, and displayed in the list of tasks.

12. To run the task, select it in the task list, and then click the **Start** button.

    You can also set a task start schedule on the **Schedule** tab of the task properties window.

    For a detailed description of scheduled start settings, refer to the general task settings.

    After the task is completed, the required updates are installed and the vulnerabilities are fixed.

If in the network of your organization the WSUS server is used (local WSUS server), and you want to use it together with Administration Server, you must first ensure that Administration Server is not used as WSUS server, and then do the following:

a. On your managed devices running Windows, specify your local WSUS server for Windows Update service. You can do it either manually in Windows Registry or by using a Windows group policy.

b. On your local WSUS server, specify the required classifications for updates and the applications on which the updates are to be distributed.

c. Synchronize your WSUS server with the upstream server (this can be either a Microsoft WSUS server, or another local upstream WSUS-server).

After the *Install required updates and fix vulnerabilities* task is run on the device, Network Agent uses the Windows Update service to install Windows updates. Windows Update service obtains the address of the external WSUS server from the registry and downloads the updates directly from that external server.

# Adding rules for update installation

This feature is only available under the Vulnerability and patch management license.

When installing software updates or fixing software vulnerabilities by using the *Install required updates and fix vulnerabilities* task, you must specify rules for the update installation. These rules determine the updates to install and the vulnerabilities to fix.

The exact settings depend on whether you add a rule for all updates, for updates from Windows Update, or for updates of third-party applications (applications made by software vendors other than Kaspersky and Microsoft). When adding a rule for updates from Windows Update or updates of third-party applications, you can select specific applications and application versions for which you want to install updates. When adding a rule for all updates, you can select the specific updates you want to install and the vulnerabilities you want to fix by installing updates.

You can add a rule for update installation in the following ways:

- By adding a rule while creating a new *Install required updates and fix vulnerabilities* task.
- By adding a rule on the **Application settings** tab in the task properties window of an existing *Install required updates and fix vulnerabilities* task.
- Through the Update installation wizard or the Vulnerability fix wizard.

Adding rules for all updates

*To add a new rule for all updates:*

1. Click **Add**.

   The Rule creation wizard starts. Proceed through the wizard by using the **Next** button.

2. At the **Select rule type** step of the wizard, select **Rule for all updates**.

3. At the **General criteria** step of the wizard, specify the following settings:

   - **Set of updates to be installed**

     Select the updates that must be installed on client devices:

     - **Install approved updates only**. This installs only approved updates.
     - **Install all updates (except declined)**. This installs updates with the *Approved* or *Undefined* approval status.
     - **Install all updates (including declined)**. This installs all updates, regardless of their approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.

   - **Fix vulnerabilities with a severity level equal to or higher than**

     Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

     If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

     If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

     By default, this option is disabled.

   Go to the next step of the wizard.

4. Select the updates to be installed:

   - **Install all suitable updates**

     Install all software updates that meet the criteria specified at the **General criteria** step of the wizard. Selected by default.

   - **Install only updates from the list**

     Install only software updates that you select manually from the list. This list contains all available software updates.

For example, you may want to select specific updates in the following cases: to check their installation in a test environment, to update only critical applications, or to update only specific applications.

- **Automatically install all previous application updates that are required to install the selected updates**

  Keep this option enabled if you agree with the installation of interim application versions when this is required for installing the selected updates.

  If this option is disabled, only the selected versions of applications are installed. Disable this option if you want to update applications in a straightforward manner, without attempting to install successive versions incrementally. If installing the selected updates is not possible without installing previous versions of applications, the updating of the application fails.

  For example, you have version 3 of an application installed on a device and you want to update it to version 5, but version 5 of this application can be installed only over version 4. If this option is enabled, the software first installs version 4, and then installs version 5. If this option is disabled, the software fails to update the application.

  By default, this option is enabled.

Go to the next step of the wizard.

5. Select the vulnerabilities that will be fixed by installing the selected updates:

   - **Fix all vulnerabilities that match other criteria**

     Fix all vulnerabilities that meet the criteria specified at the **General criteria** step of the wizard. Selected by default.

   - **Fix only vulnerabilities from the list**

     Fix only vulnerabilities that you select manually from the list. This list contains all detected vulnerabilities.

     For example, you may want to select specific vulnerabilities in the following cases: to check their fix in a test environment, to fix vulnerabilities only in critical applications, or to fix vulnerabilities only in specific applications.

   Go to the next step of the wizard.

6. Specify the name of the rule that you are adding. You can later change this name on the **Application settings** tab in the task properties window of the created task.

The new rule is created, configured, and displayed in the table of rules of the New task wizard.

## Adding rules for updates from Windows Update

*To add a new rule for updates from Windows Update:*

1. Click **Add**.

   The Rule creation wizard starts. Proceed through the wizard by using the **Next** button.

2. Select **Rule for Windows Update**.

   Go to the next step of the wizard.

3. At the **General criteria** step of the wizard, specify the following settings:

   - **Set of updates to be installed**

     Select the updates that must be installed on client devices:

     - **Install approved updates only**. This installs only approved updates.
     - **Install all updates (except declined)**. This installs updates with the *Approved* or *Undefined* approval status.
     - **Install all updates (including declined)**. This installs all updates, regardless of their approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.

   - **Fix vulnerabilities with a severity level equal to or higher than**

     Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

     If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

     If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

     By default, this option is disabled.

   - **Fix vulnerabilities with an MSRC severity level equal to or higher than**

     Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

     If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Microsoft Security Response Center (MSRC) is equal to or higher than the value selected in the list (**Low**, **Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

     If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

     By default, this option is disabled.

4. On the **Applications** page, select the applications and application versions for which you want to install updates. By default, all applications are selected.

5. On the **Categories of updates** page, select the categories of updates to be installed. These categories are the same as in Microsoft Update Catalog. By default, all categories are selected.

6. On the **Name** page, specify the name for the rule that you are adding. You can later change this name in the **Settings** section of the properties window of the created task.

After the Rule creation wizard completes its operation, the new rule is added and displayed in the rule list in the New task wizard or in the task properties.

## Adding rules for updates of third-party applications

*To add a new rule for updates of third-party applications:*

1. Click **Add**.

   The Rule creation wizard starts. Proceed through the wizard by using the **Next** button.

2. At the **Select rule type** step of the wizard, select **Rule for third-party updates**.

3. At the **General criteria** step of the wizard, specify the following settings:

   - **Set of updates to be installed**

     Select the updates that must be installed on client devices:

     - **Install approved updates only**. This installs only approved updates.
     - **Install all updates (except declined)**. This installs updates with the *Approved* or *Undefined* approval status.
     - **Install all updates (including declined)**. This installs all updates, regardless of their approval status. Select this option with caution. For example, use this option if you want to check installation of some declined updates in a test infrastructure.

   - **Fix vulnerabilities with a severity level equal to or higher than**

     Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

     If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the value selected in the list (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

     If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

     By default, this option is disabled.

   Go to the next step of the wizard.

4. Select the applications and application versions for which you want to install updates.

   By default, all applications are selected.

   Go to the next step of the wizard.

5. Specify the name of the rule that you are adding. You can later change this name on the **Application settings** tab in the task properties window of the created task.

The new rule is created, configured, and displayed in the table of rules of the New task wizard.

# Settings of the Install required updates and fix vulnerabilities task specified after task creation

After the creation of the *Install required updates and fix vulnerabilities* task, you can specify the following settings on the **Application settings** tab of the task properties window:

- In the **Test installation** section:

  - **Do not scan**. Select this option if you do not want to perform a test installation of updates.
  - **Run scan on selected devices**. Select this option if you want to test the updates installation on selected devices. Click the **Add** button, and then select the devices on which you need to perform a test installation of updates.

- **Run scan on devices in the specified group**. Select this option if you want to test the updates installation on a group of devices. In the **Specify a test group** field, specify a group of devices on which you want to perform a test installation.

- **Run scan on specified percentage of devices**. Select this option if you want to test the updates installation on a percentage of devices. In the **Percentage of test devices out of all target devices** field, specify the percentage of devices on which you want to perform a test installation of updates.

Upon selecting any option other than **Do not scan**, in the **Amount of time to make the decision if the installation is to be continued, in hours** field, specify the number of hours that must elapse from the test installation of updates until the start of installation of the updates on all devices.

- In the **Updates to install** section, you can view the list of updates that the task installs. Only updates that match the applied task settings are shown.

For a full description of task settings, refer to the general task settings.

# Updating third-party applications automatically

Some third-party applications can be updated automatically. The application vendor defines whether the application supports the auto-update feature. If a third-party application installed on a managed device supports auto-update, you can specify the auto-update setting in the application properties. After you change the auto-update setting, Network Agents apply the new setting on each managed device on which the application is installed.

The auto-update setting is independent of the other objects and settings of the Vulnerability and patch management feature. For example, this setting does not depend on an update approval status or the update installation tasks, such as *Install required updates and fix vulnerabilities* and *Fix vulnerabilities*.

*To configure the auto-update setting for a third-party application:*

1. In the main application window, go to the **Software management** → **Third-party applications** → **Applications registry** section.

2. Click the name of the application for which you want to change the auto-update setting.

   To simplify the search, you can filter the list by the **Automatic Updates status** and **Manage Automatic Updates** columns.

   The application properties window opens.

3. In the **General** section, select a value for the following feature:

   **Automatic Updates status**

   Choose one of the following options:

   - **Undefined**

     The auto-update feature is disabled. Kaspersky Security Center Linux installs third-party application updates by using the tasks: *Install required updates and fix vulnerabilities* and *Fix vulnerabilities*.

   - **Allowed**

     After the vendor releases an update for the application, this update is installed on the managed devices automatically. No additional actions required.

- **Blocked**

  The application updates are not installed automatically. Kaspersky Security Center Linux installs third-party application updates by using the tasks: *Install required updates and fix vulnerabilities* and *Fix vulnerabilities*.

4. Click **Save** to save the changes.

The auto-update setting is applied to the selected application.

# Fixing third-party software vulnerabilities

This section describes the features of Kaspersky Security Center Linux that relate to fixing vulnerabilities in the software installed on managed devices.

## About finding and fixing software vulnerabilities

Kaspersky Security Center Linux detects and fixes software vulnerabilities on managed devices running Microsoft Windows operating systems. Vulnerabilities are detected in the operating system and in third-party software, including Microsoft software.

> Updates functionality (including providing anti-virus signature updates and codebase updates), as well as KSN functionality may not be available in the software in the U.S.

### Finding software vulnerabilities

To find software vulnerabilities, Kaspersky Security Center Linux uses characteristics from the database of known vulnerabilities. This database was created and is kept up-to-date by Kaspersky specialists. It contains information about vulnerabilities, such as vulnerability description, vulnerability detection date, and vulnerability severity level. You can find the details of software vulnerabilities on the Kaspersky website.

Kaspersky Security Center Linux uses the *Find vulnerabilities and required updates* task to find software vulnerabilities.

### Fixing software vulnerabilities

To fix software vulnerabilities, Kaspersky Security Center Linux uses software updates issued by software vendors. The metadata of the software updates is downloaded to the Administration Server repository as the result of running the *Download updates to the Administration Server repository* task. This task is intended to download the metadata for Kaspersky and third-party software updates. This task is created automatically by the Kaspersky Security Center Linux quick start wizard. You can also create the *Download updates to the Administration Server repository* task manually.

Software updates to fix vulnerabilities can be represented as full distribution packages or patches. Software updates that fix software vulnerabilities are named *fixes*. *Recommended fixes* are those that are recommended for installation by Kaspersky specialists. *User fixes* are those that are manually specified for installation by users. To install a user fix, you have to create an installation package containing this fix.

If you have the Kaspersky Security Center Linux license with the Vulnerability and patch management feature, you can use the *Install required updates and fix vulnerabilities* task. This task automatically fixes multiple vulnerabilities by installing recommended fixes. For this task, you can manually configure certain rules to fix multiple vulnerabilities.

If you do not have the Kaspersky Security Center Linux license with the Vulnerability and patch management feature, you can use the *Fix vulnerabilities* task. By using this task, you can fix vulnerabilities by installing recommended fixes for Microsoft software and user fixes for other third-party software.

For security reasons, any third-party software updates that you install by using the Vulnerability and patch management feature are automatically scanned for malware by Kaspersky technologies. These technologies are used for automatic file checks and include virus scanning, static analysis, dynamic analysis, behavior analysis in the sandbox environment, and machine learning.

Kaspersky experts do not perform manual analysis of third-party software updates that can be installed by using the Vulnerability and patch management feature. In addition, Kaspersky experts do not search for vulnerabilities (known or unknown) or undocumented features in such updates, nor do they perform other types of analysis of the updates other than those specified in the paragraph above.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it is currently open.

To fix some software vulnerabilities, you must accept the End User License Agreement (EULA) for installing the software if EULA acceptance is requested. If you decline the EULA, the software vulnerability is not fixed.

# Scenario: Finding and fixing third-party software vulnerabilities

This section provides a scenario for finding and fixing vulnerabilities on the managed devices running Windows. You can detect and fix vulnerabilities in the operating system and in third-party software, including Microsoft software.

Prerequisites

- Kaspersky Security Center Linux is deployed in your organization.
- There are managed devices running Windows in your organization.
- An internet connection is required for the Administration Server to perform the following tasks:
  - To make a list of recommended fixes for vulnerabilities in Microsoft software. The list is created and regularly updated by Kaspersky specialists.
  - To fix vulnerabilities in third-party software other than Microsoft software.

## Stages

Finding and fixing software vulnerabilities proceeds in stages:

1. **Scanning for vulnerabilities in the software installed on the managed devices**

   To find vulnerabilities in the software installed on managed devices, run the *Find vulnerabilities and required updates* task. When this task is complete, Kaspersky Security Center Linux receives a list of detected vulnerabilities and the required updates for the third-party software installed on the devices that you specified in the task properties.

   The *Find vulnerabilities and required updates* task is created automatically by the Kaspersky Security Center Linux quick start wizard. If you did not run the wizard, start it now or create the task manually.

   > You can create the *Find vulnerabilities and required updates* task only for Windows devices. You cannot create this task for devices running on other operating systems.

2. **Viewing the list of detected software vulnerabilities**

   View the **Software vulnerabilities** list and decide which vulnerabilities need to be fixed. To view detailed information about each vulnerability, click the vulnerability name in the list. For each vulnerability in the list, you can also view the statistics on the vulnerability on managed devices.

3. **Configuring vulnerabilities fix**

   When software vulnerabilities are detected, you can fix them on managed devices by using the *Install required updates and fix vulnerabilities* task or the *Fix vulnerabilities* task.

   The *Install required updates and fix vulnerabilities* task is used to update and fix vulnerabilities in third-party software, including Microsoft software, installed on managed devices. This task enables you to install multiple updates and fix multiple vulnerabilities according to certain rules. Note that this task can be created only if you have the license for the Vulnerability and patch management feature. To fix software vulnerabilities, the *Install required updates and fix vulnerabilities* task uses recommended software updates.

   The *Fix vulnerabilities* task does not require the license option for the Vulnerability and patch management feature. To use this task, you must manually specify user fixes for the vulnerabilities in the third-party software listed in the task settings. The *Fix vulnerabilities* task uses the recommended fixes for Microsoft software and user fixes for third-party software.

   > You can create the *Install required updates and fix vulnerabilities* task and *Fix vulnerabilities* task only for Windows devices. You cannot create these tasks for devices running on other operating systems.

   You can start the Vulnerability fix wizard that creates one of these tasks automatically, or you can create one of these tasks manually.

   If you have created and configured the *Install required updates and fix vulnerabilities* task, the vulnerabilities are fixed on managed devices automatically. When the created task is started, it correlates the list of available software updates to the rules specified in the task settings. All software updates that meet the criteria in the specified rules are downloaded to the Administration Server repository and installed to fix software vulnerabilities.

   If you have created the *Fix vulnerabilities* task, only vulnerabilities for Microsoft software are fixed.

4. **Scheduling the tasks**

   Schedule the *Find vulnerabilities and required updates* task to run automatically on a periodic basis to keep the list of vulnerabilities up-to-date. The recommended frequency is once a week.

If you have created the *Install required updates and fix vulnerabilities* task, you can schedule it to run with the same frequency as the *Find vulnerabilities and required updates* task or less often. When scheduling the *Fix vulnerabilities* task, note that you have to select fixes for Microsoft software or specify user fixes for third-party software every time before starting the task.

When scheduling the tasks, make sure that a task created to fix vulnerabilities starts after the *Find vulnerabilities and required updates* task is complete.

5. **Ignoring software vulnerabilities (optional)**

   You can ignore certain software vulnerabilities on all managed devices or only on selected managed devices.

6. **Running a vulnerability fix task**

   Start the *Install required updates and fix vulnerabilities* task or the *Fix vulnerabilities* task. When the task is complete, make sure that it has the *Completed successfully* status in the task list.

7. **Create the report on results of fixing software vulnerabilities (optional)**

   To view detailed statistics on the vulnerabilities fixed, generate the Report on vulnerabilities. This report displays information about software vulnerabilities that are not fixed. It allows you to identify and address vulnerabilities in third-party software, including Microsoft software, that is used in your organization.

8. **Checking configuration of finding and fixing vulnerabilities in third-party software**

   Be sure that you have done the following:

   - Obtained and reviewed the list of software vulnerabilities on managed devices.
   - Ignored certain software vulnerabilities, if desired.
   - Configured the task to fix vulnerabilities.
   - Scheduled the tasks to find and fix software vulnerabilities so that they start sequentially.
   - Checked that the task to fix software vulnerabilities has started.

# Fixing third-party software vulnerabilities

To find third-party software vulnerabilities, you can create and run the *Find vulnerabilities and required updates* task and receive a list of software vulnerabilities. After you obtain the software vulnerabilities list, you can fix the vulnerabilities on the managed devices that are running Windows.

You can fix software vulnerabilities in the operating system and in third-party software, including Microsoft software, by creating and running the Fix vulnerabilities task or the Install required updates and fix vulnerabilities task.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it is currently open.

As an option, you can create a task to fix software vulnerabilities in the following ways:

- By opening the vulnerability list and specifying which vulnerabilities to fix.

  As a result, a new task to fix software vulnerabilities is created. As an option, you can add the selected vulnerabilities to an existing task.

- By running the Vulnerability fix wizard.

  > The Vulnerability fix wizard is only available under the Vulnerability and patch management license.

  The wizard simplifies the creation and configuration of a vulnerability fix task, and allows you to eliminate the creation of redundant tasks.

### Fixing software vulnerabilities by using the vulnerability list

*To fix software vulnerabilities by using the vulnerability list:*

1. Open the list of vulnerabilities by doing one of the following:

   - In the main menu, go to **Software management** → **Patch management** → **Software vulnerabilities**.
   - In the main menu, go to **Asset management** → **Managed devices** → <device name> → **Advanced** → **Software vulnerabilities**.
   - In the main application window, go to the **Software management** → **Third-party applications** → **Applications registry** → <application name> → **Vulnerabilities** section.

   A table with the list of vulnerabilities in the third-party software installed on managed devices is displayed.

2. In the list of vulnerabilities, select the check boxes next to the vulnerabilities you want to fix, and then click the **Fix vulnerability** button.

   If a recommended software update to fix one of the selected vulnerabilities is absent, an informative message is displayed.

   To fix some software vulnerabilities, you must accept the End User License Agreement (EULA) for installing the software, if EULA acceptance is requested. If you decline the EULA, the software vulnerability is not fixed.

3. Choose one of the following options:

   - **New task**

     The New task wizard starts. If you have the Vulnerability and patch management license, the Install required updates and fix vulnerabilities task is preselected. If you do not have the license, the Fix vulnerabilities task is preselected. Follow the steps of the wizard to complete the task creation.

   - **Fix vulnerability (add rule to specified task)**

     Select a task to which you want to add the selected vulnerabilities. If you have the Vulnerability and patch management license, select the Install required updates and fix vulnerabilities task. A new rule to fix the selected vulnerabilities will be automatically added to the selected task. If you do not have the license, select the Fix vulnerabilities task. The selected vulnerabilities are added to the task properties.

     The task properties window opens. Click **Save** to save the changes.

   If you have chosen to create a task, the task is created and displayed in the task list at **Tasks**. If you have chosen to add the vulnerabilities to an existing task, the vulnerabilities are saved in the task properties.

To fix the third-party software vulnerabilities, start the Install required updates and fix vulnerabilities task or the Fix vulnerabilities task. If you have created the Fix vulnerabilities task, you must manually specify the software updates listed in the task settings.

Fixing software vulnerabilities by using the Vulnerability fix wizard

The Vulnerability fix wizard is only available under the Vulnerability and patch management license.

*To fix software vulnerabilities by using the Vulnerability fix wizard:*

1. In the main menu, go to **Software management** → **Patch management** → **Software vulnerabilities**.

   A table with a list of vulnerabilities in the third-party software installed on managed devices is displayed.

2. Select the check box next to the vulnerability that you want to fix.

3. Click the **Run Vulnerability fix wizard** button.

   The button is disabled if you select more than one vulnerability.

   The Vulnerability fix wizard starts. The list of existing tasks is displayed. This list may contain the following types of tasks:

   - Install required updates and fix vulnerabilities
   - Fix vulnerabilities

   You cannot modify the Fix vulnerabilities task to install new updates. To install new updates, you can only use the Install required updates and fix vulnerabilities task.

4. If you want the wizard to display only those tasks that fix the vulnerability that you selected, enable the **Show only tasks that fix this vulnerability** option.

5. Do one of the following:

   - To start a task, select the check box next to the task name, and then click the **Start** button.

     No further actions are required. You can close the wizard. The task will complete in background mode.

   - To add a new rule to an existing Install required updates and fix vulnerabilities task:

     a. Select the check box next to the task name, and then click the **Add rule** button.

     The **Add rule** button is disabled if you select more than one task.

     You cannot add a rule for a Fix vulnerabilities task. If you select a Fix vulnerabilities task, the following notification is displayed: "To install updates, use the "Install required updates and fix vulnerabilities" task."

     b. On the page that opens, configure the new rule:

     - **Rule for fixing vulnerabilities of this severity level**

       Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the severity of the selected update (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

By default, this option is disabled.

- **Rule for fixing vulnerabilities by means of updates of the same type as the update defined as recommended for the selected vulnerability**

  This rule is displayed only for Microsoft software vulnerabilities.

- **Rule for fixing vulnerabilities in applications from the selected vendor**

  This rule is displayed only for third-party software vulnerabilities.

- **Rule for fixing a vulnerability in all versions of the selected application**

  This rule is displayed only for third-party software vulnerabilities.

- **Rule for fixing the selected vulnerability**

- **Approve updates that fix this vulnerability**

  The selected update will be approved for installation. Enable this option if some applied rules of update installation allow installation of approved updates only.

  By default, this option is disabled.

c. Click **Add**.

The task properties window opens. The new rule is already added to the task properties. You can view or modify the rule, or other task settings. Click **Save** to save the changes.

- To create a task:

  a. Click the **New task** button.

  b. On the page that opens, configure the new rule:

  - **Rule for fixing vulnerabilities of this severity level**

    Sometimes software updates may impair the user experience with the software. In such cases, you may decide to install only those updates that are critical for the software operation and to skip other updates.

    If this option is enabled, the updates fix only those vulnerabilities for which the severity level set by Kaspersky is equal to or higher than the severity of the selected update (**Medium**, **High**, or **Critical**). Vulnerabilities with a severity level lower than the selected value are not fixed.

    If this option is disabled, the updates fix all vulnerabilities regardless of their severity level.

    By default, this option is disabled.

  - **Rule for fixing vulnerabilities by means of updates of the same type as the update defined as recommended for the selected vulnerability**

    This rule is displayed only for Microsoft software vulnerabilities.

  - **Rule for fixing vulnerabilities in applications from the selected vendor**

    This rule is displayed only for third-party software vulnerabilities.

- **Rule for fixing a vulnerability in all versions of the selected application**

  This rule is displayed only for third-party software vulnerabilities.

- **Rule for fixing the selected vulnerability**

- **Approve updates that fix this vulnerability**

  The selected update will be approved for installation. Enable this option if some applied rules of update installation allow installation of approved updates only.

  By default, this option is disabled.

c. Click **Add**.

d. Continue to create the task in the New task wizard.

The new rule that you added in the Vulnerability fix wizard is displayed at the **Specify rules for installing updates** step of the New task wizard. When you complete the wizard, the Install required updates and fix vulnerabilities task is added to the task list.

# Creating the Fix vulnerabilities task

The *Fix vulnerabilities* task allows you to fix software vulnerabilities on managed devices. You can fix software vulnerabilities in third-party software, including Microsoft software.

You can create the *Fix vulnerabilities* task only for Windows devices. You cannot create this task for devices running on other operating systems.

You can create new *Fix vulnerabilities* tasks only if you have the Vulnerability and patch management license.

To fix new vulnerabilities, you can add them to an existing *Fix vulnerabilities* task. However, we recommend that you use the *Install required updates and fix vulnerabilities* task instead of the *Fix vulnerabilities* task. The *Install required updates and fix vulnerabilities* task enables you to install multiple updates and fix multiple vulnerabilities automatically, according to the rules that you define.

A user interaction may be required when you update a third-party application or fix a vulnerability in a third-party application on a managed device. For example, the user may be prompted to close the third-party application if it is currently open.

*To create the Fix vulnerabilities task:*

1. In the main menu, go to **Tasks**.

   Alternatively, you can create this task in the device properties window on the **Tasks** tab.

2. Click **Add**.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.

3. In the **Application** drop-down list, select Kaspersky Security Center.

4. In the **Task type** list, select the **Fix vulnerabilities** task type.

5. In the **Task name** field, specify the name of the new task.

   The task name cannot be more than 100 characters long and cannot include any special characters ("*<>?\:|).

6. Select devices to which the task will be assigned.

   Go to the next step of the wizard.

7. Click **Add**.

   The list of vulnerabilities opens.

8. In the list of vulnerabilities, select the check boxes next to the vulnerabilities you want to fix, and then click the **OK** button.

   Microsoft software vulnerabilities usually have recommended fixes. No additional actions are required for them.

   For vulnerabilities in software from other vendors, you first need to specify a user fix for each vulnerability that you want to fix. After that, you will be able to add those vulnerabilities to the *Fix vulnerabilities* task.

   Go to the next step of the wizard.

9. Specify the operating system restart settings:

   - **Do not restart the device**

     Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

   - **Restart the device**

     Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

   - **Prompt user for action**

     The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

     By default, this option is selected.

   - **Repeat prompt every (min)**

     If this option is enabled, the application prompts the user to restart the operating system with the specified frequency.

     By default, the option is enabled. The default interval is 5 minutes. Available values are between 1 and 1440 minutes.

     If this option is disabled, the prompt is displayed only once.

   - **Restart after (min)**

     After prompting the user, the application forces restart of the operating system upon expiration of the specified time interval.

By default, the option is enabled. The default delay is 30 minutes. Available values are between 1 and 1440 minutes.

- **Force closure of applications in blocked sessions**

  Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

  If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

  If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

  By default, this option is disabled.

Go to the next step of the wizard.

10. Specify the account settings:

    - **Default account**

      The task will be run under the same account as the application that performs this task.

      By default, this option is selected.

    - **Specify account**

      Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

    - **Account**

      Account under which the task is run.

    - **Password**

      Password of the account under which the task will be run.

11. At the **Finish task creation** step of the wizard, enable the **Open task details when creation is complete** option to modify the default task settings.

    If you do not enable this option, the task is created with the default settings. You can modify the default settings later.

12. Click the **Finish** button.

    The wizard creates the task. If you enabled the **Open task details when creation is complete** option, the task properties window automatically opens. In this window, you can specify the general task settings and, if required, change the settings specified during task creation.

    > You can also open the task properties window by clicking the name of the created task in the list of tasks.

    The task is created, configured, and displayed in the list of tasks at **Tasks**.

13. To run the task, select it in the task list, and then click the **Start** button.

    You can also set a task start schedule on the **Schedule** tab of the task properties window.

    For a detailed description of scheduled start settings, refer to the general task settings.

After the task is completed, the selected vulnerabilities are fixed.

# Selecting user fixes for vulnerabilities in third-party software

To use the *Fix vulnerabilities* task, you must manually specify the software updates to fix the vulnerabilities in third-party software listed in the task settings. The *Fix vulnerabilities* task uses recommended fixes for Microsoft software and user fixes for other third-party software.

*User fixes* are software updates that the administrator manually specifies for installation to fix vulnerabilities.

*To select user fixes for vulnerabilities in third-party software:*

1. In the main menu, go to **Software management** → **Patch management** → **Software vulnerabilities**.

   A table with the list of vulnerabilities in the third-party software installed on managed devices is displayed.

2. In the list of software vulnerabilities, click the link with the name of the software vulnerability for which you want to specify a user fix.

   The properties window of the selected vulnerability opens.

3. In the left pane, select the **User fixes and other fixes** section.

   The list of user fixes for the selected software vulnerability is displayed.

4. Click **Add**.

   The list of available installation packages is displayed. The list of displayed installation packages corresponds to the list in the **Software management** → **Installation packages** folder.

   If you have not created an installation package containing a user fix for the selected vulnerability, you can create the package now by clicking the **New** button, and then going through the New package wizard.

5. Select an installation package (or packages) containing a user fix (or user fixes) for the selected vulnerability.

6. Click the **Save** button.

The installation packages containing user fixes for the software vulnerability are specified. When you start the *Fix vulnerabilities* task, the installation package is installed, and the software vulnerability is fixed.

# Viewing information about software vulnerabilities detected on all managed devices

After you have scanned the software on managed devices for vulnerabilities, you can view the list of detected software vulnerabilities. If you run the task for the hierarchy of Administration Servers, you can view the list of managed devices with detected vulnerabilities only for the selected Administration Server.

You can also generate and view a Report on vulnerabilities.

*To view the list of software vulnerabilities detected on all managed devices,*

In the main menu, go to **Operations** → **Patch management** → **Software vulnerabilities**.

The list of software vulnerabilities detected on client devices is displayed.

*To adjust the list of software vulnerabilities,*

Click the **Filter** icon ( ) in the upper right corner of the software vulnerabilities list, and then select the filters you need. You can also select one of the preset filters from the **Preset filters** drop-down list above the software vulnerabilities list.

You can obtain detailed information about any vulnerability from the list.

*To obtain information about a software vulnerability,*

In the list of software vulnerabilities, click the link with the name of the vulnerability.

The properties window of the software vulnerability opens.

# Viewing information about software vulnerabilities detected on the selected managed device

You can view information about software vulnerabilities detected on the selected managed device running Windows.

*To view the list of software vulnerabilities detected on the selected managed device:*

1. In the main menu, go to **Asset management** → **Managed devices**.

   The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the device for which you want to view detected software vulnerabilities.

   The properties window of the selected device is displayed.

3. In the properties window of the selected device, select the **Advanced** tab.

4. In the left pane, select the **Software vulnerabilities** section.

The list of software vulnerabilities detected on the selected managed device is displayed.

*To view the properties of the selected software vulnerability,*

Click the link with the name of the software vulnerability in the list of software vulnerabilities.

The properties window of the selected software vulnerability is displayed.

# Viewing statistics of vulnerabilities on managed devices

You can view statistics for each software vulnerability on managed devices. Statistics are represented as a diagram. The diagram displays the number of devices with the following statuses:

- *Ignored on: <number of devices>*. This status is assigned if, in the vulnerability properties, you have manually set the option to ignore the vulnerability.
- *Fixed on: <number of devices>*. This status is assigned if the task to fix the vulnerability has successfully completed.
- *Fix scheduled on: <number of devices>*. This status is assigned if you have created the task to fix the vulnerability, but the task is not performed yet.
- *Patch applied on: <number of devices>*. This status is assigned if you have manually selected a software update to fix the vulnerability, but this software update has not fixed the vulnerability.
- *Fix required on: <number of devices>*. This status is assigned if the vulnerability was fixed only on some managed devices, and the vulnerability is required to be fixed on more managed devices.

*To view the statistics of a vulnerability on managed devices:*

1. In the main menu, go to **Operations → Patch management → Software vulnerabilities**.

   The page displays a list of vulnerabilities for the applications detected on managed devices.

2. Select the check box next to a vulnerability.
3. Click the **Statistics of vulnerability on devices** button.

   The **Statistics of vulnerability on devices** button is disabled if you select more than one vulnerability.

A diagram of the vulnerability statuses is displayed. Clicking a status opens a list of devices on which the vulnerability has the selected status.

# Exporting the list of software vulnerabilities to a file

You can download the displayed list of vulnerabilities as a CSV or TXT file. You can send these files to your information security manager or store them for purposes of statistics.

*To export the list of software vulnerabilities detected on all managed devices to a text file:*

1. In the main menu, go to **Operations → Patch management → Software vulnerabilities**.

   A list of software vulnerabilities in the applications detected on managed devices is displayed.

   By default, only vulnerabilities displayed on the current page are exported.

If you want to export only specific vulnerabilities, select the check boxes next to those vulnerabilities.

2. Click the **Export to TXT** or **Export to CSV** button, depending on the format you prefer. If either of these buttons is not visible, click the ellipsis button, and then select the required option from the drop-down list.

A file containing the list of software vulnerabilities is downloaded to your device.

*To view the list of software vulnerabilities detected on the selected managed device:*

1. In the main menu, go to **Asset management** → **Managed devices**.

   The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the device for which you want to view detected software vulnerabilities.

   The properties window of the selected device is displayed.

3. In the properties window of the selected device, select the **Advanced** tab.

4. In the left pane, select the **Software vulnerabilities** section.

The list of software vulnerabilities detected on the selected managed device is displayed.

By default, only vulnerabilities displayed on the current page are exported.

If you want to export only specific vulnerabilities, select the check boxes next to those vulnerabilities.

1. Click the **Export to TXT** or **Export to CSV** button, depending on the format you prefer. If either of these buttons is not visible, click the ellipsis button, and then select the required option from the drop-down list.

A file containing the list of software vulnerabilities is downloaded to your device.

# Ignoring software vulnerabilities

You can ignore software vulnerabilities to be fixed. The reasons to ignore software vulnerabilities might be, for example, the following:

- You do not consider the software vulnerability to be critical to your organization.
- You understand that the software vulnerability fix can damage data related to the software that required the vulnerability fix.
- You are sure that the software vulnerability is not dangerous for your organization's network because you use other measures to protect your managed devices.

You can ignore a software vulnerability on all managed devices or only on selected managed devices.

*To ignore a software vulnerability on all managed devices:*

1. In the main menu, go to **Operations** → **Patch management** → **Software vulnerabilities**.

   A list of software vulnerabilities in the applications detected on managed devices is displayed.

2. In the list of software vulnerabilities, click the link with the name of the software vulnerability you want to ignore.

   The properties window of the software vulnerability opens.

3. On the **General** tab, enable the **Ignore vulnerability** option.
4. Click the **Save** button.

   The software vulnerability properties window is closed.

The software vulnerability is ignored on all managed devices.

*To ignore a software vulnerability on a selected managed device:*

1. In the main menu, go to **Asset management** → **Managed devices**.

   The list of managed devices is displayed.
2. In the list of managed devices, click the link with the name of the device on which you want to ignore a software vulnerability.

   The device properties window is opened.
3. In the device properties window, select the **Advanced** tab.
4. In the left pane, select the **Software vulnerabilities** section.

   The list of software vulnerabilities detected on the device is displayed.
5. In the list of software vulnerabilities, select the vulnerability you want to ignore on the selected device.

   The properties window of the software vulnerability opens.
6. In the software vulnerability properties window, on the **General** tab, enable the **Ignore vulnerability** option.
7. Click the **Save** button.

   The software vulnerability properties window is closed.
8. Close the device properties window.

The software vulnerability is ignored on the selected device.

The ignored software vulnerability will not be fixed after the completion of the *Fix vulnerabilities* task or *Install required updates and fix vulnerabilities* task. You can exclude ignored software vulnerabilities from the list of vulnerabilities by using a filter.

# Creating an installation package of a third-party application from the Kaspersky database

Kaspersky Security Center Web Console allows you to perform remote installation of third-party applications by using installation packages. Such third-party applications are included in a dedicated Kaspersky database. This database is created automatically when you run the *Download updates to the Administration Server repository task* for the first time.

> You can create an installation package of a third-party application from the Kaspersky database only if you have a Vulnerability and patch management license.

*To create an installation package of a third-party application from the Kaspersky database:*

1. In the main menu, go to the **Software management** → **Installation packages** section.
2. Click **Add**.

   The New package wizard starts. Proceed through the wizard by using the **Next** button.
3. Select the **Select an application from the Kaspersky database to create an installation package** option.

   This option is only available under the Vulnerability and patch management license.

   Go to the next step of the wizard.
4. Select the application for which you want to create an installation package.

   Go to the next step of the wizard.
5. Select the relevant localization language in the drop-down list, and then click Next.

   This step is only displayed if the application offers multiple language options.
6. If you are prompted to accept a License Agreement for the installation, at the **License Agreements and Privacy Policies** step of the wizard, do the following:

   a. Click the **Show** link to read the License Agreement on the vendor's website or view updates with the license.

   b. Select the **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement** check box.

   c. Click the **Accept all** button to accept all license agreements and privacy policies that are displayed in the list.
7. At the **Name of the new installation package** step of the wizard, in the **Package name**, enter the name for the installation package, and then click **Next**.

   The newly created installation package is uploaded to the Administration Server. The New package wizard displays a message informing you that the installation package has been successfully created.
8. Click the **Finish** button.

The newly created installation package is displayed in the list of installation packages. You can select this package when creating or reconfiguring the Install application remotely task.

You can create and reconfigure the Install application remotely task by using an installation package of a third-party application from the Kaspersky database only if you have a Vulnerability and patch management license.

# Viewing and modifying the settings of an installation package of a third-party application from the Kaspersky database

If you have previously created any installation packages of third-party applications listed in the Kaspersky database, you can subsequently view and modify the settings of these packages.

Modifying the settings of an installation package of a third-party application from the Kaspersky database is only available under the Vulnerability and patch management license.

*To view and modify the settings of an installation package of a third-party application from the Kaspersky database:*

1. In the main menu, go to **Software management** → **Installation packages**.
2. In the list of installation packages that opens, click the name of the relevant package.

   The properties window opens.
3. Adjust settings if necessary.
4. Click the **Save** button.

   The settings that you modified are saved.

# Settings of an installation package of a third-party application from the Kaspersky database

The settings of an installation package for a third-party application are grouped on the following tabs:

Not all of the settings listed below are displayed by default. You can add the columns you need by clicking the **Filter** button, and then selecting relevant column names from the list.

- **General** tab:
  - Entry field that contains the name of the installation package and which can be edited manually
  - **Application**

    The name of the third-party application for which the installation package is created.
  - **Version**

    The version number of the third-party application for which the installation package is created.

- **Size**

  The size of the third-party installation package (in kilobytes).

- **Created**

  The date and time the third-party installation package was created.

- **Path**

  The path to the network folder where the third-party installation package is stored.

- **Installation procedure** tab:

  - **Install the required general system components**

    If this option is enabled, before installing an update the application automatically installs all general system components (prerequisites) that are required to install the update. For example, these prerequisites can be operating system updates.

    If this option is disabled, you may have to install the prerequisites manually.

    By default, this option is disabled.

  - Table that displays the update properties and contains the following columns:

    - **Name**

      The name of the update.

    - **Description**

      The description of the update.

    - **Source**

      The source of the update, that is, whether it was released by Microsoft or by a different third-party developer.

    - **Type**

      The type of the update, that is, whether it is intended for a driver or an application.

    - **Category**

      The Windows Server Update Services (WSUS) category displayed for Microsoft updates (Critical Updates, Definition Updates, Drivers, Feature Packs, Security Updates, Service Packs, Tools, Update Rollups, Updates, or Upgrade).

    - **Importance level according to MSRC**

      The importance level of the update defined by Microsoft Security Response Center (MSRC).

    - **Importance level**

      The importance level of the update defined by Kaspersky.

    - **Patch importance level**

      The importance level of the patch if it is intended for a Kaspersky application.

- **Article**

  The identifier (ID) of the article in the Knowledge Base describing the update.

- **Bulletin**

  The ID of the security bulletin describing the update.

- **Not assigned for installation (new version)**

  Displays whether the update has the Not assigned for installation status.

- **To be installed**

  Displays whether the update has the To be installed status.

- **Installing**

  Displays whether the update has the Installing status.

- **Installed**

  Displays whether the update has the Installed status.

- **Failed**

  Displays whether the update has the Failed status.

- **Restart is required**

  Displays whether the update has the Restart is required status.

- **Registered**

  Displays the date and time when the update was registered.

- **Installed in interactive mode**

  Displays whether the update requires interaction with the user during installation.

- **Update approval status**

  Displays whether the update is approved for installation.

- **Revision**

  Displays the current revision number of the update.

- **Update ID**

  Displays the ID of the update.

- **Application version**

  Displays the version number to which the application is to be updated.

- **Superseded**

  Displays other update(s) that can supersede the update.

- **Superseding**

  Displays other update(s) that can be superseded by the update.

- **You must accept the terms of the License Agreement**

  Displays whether the update requires acceptance of the terms of an End User License Agreement (EULA).

- **Description URL**

  Displays the name of the update vendor.

- **Application family**

  Displays the name of the family of applications to which the update belongs.

- **Application**

  Displays the name of the application to which the update belongs.

- **Localization language**

  Displays the language of the update localization.

- **Not assigned for installation (new version)**

  Displays whether the update has the Not assigned for installation (new version) status.

- **Requires prerequisites installation**

  Displays whether the update has the Requires prerequisites installation status.

- **Download mode**

  Displays the mode of the update download.

- **Is a patch**

  Displays whether the update is a patch.

- **Not installed**

  Displays whether the update has the Not installed status.

- **Created**

- **Settings** tab that displays the installation package settings with their names, descriptions, and values used as command-line parameters during installation. If the package provides no such settings, a corresponding message is displayed. You can modify the values of these settings.

- **Revision history** tab that displays the installation package revisions and contains the following columns:

  - **Revision**—The number of the installation packages revision.

  - **Time**—Date and time the installation package settings were modified.

  - **User**—Name of the user who modified the installation package settings.

- **User device IP address**—IP address of the device from which the object was modified.
- **Web Console IP address**—IP address of Kaspersky Security Center Web Console with which the object was modified.
- **Action**—Action performed on the installation package within the revision.
- **Description**—Description of the revision related to the change made to the installation package settings.

  By default, the revision description is blank. To add a description to a revision, select the relevant revision and click the **Edit description** button. In the opened window, enter some text for the revision description.

# Fixing vulnerabilities in an isolated network

This section describes the steps that you can take to fix third-party software vulnerabilities on managed devices connected to Administration Servers that do not have internet access.

## Scenario: Fixing third-party software vulnerabilities in an isolated network

You can install updates and fix vulnerabilities of the third-party software installed on managed devices in an isolated network. Such networks include Administration Servers and managed devices connected to them that have no internet access. To fix vulnerabilities in this kind of network, you need an Administration Server connected to the internet. By using the Administration Server with internet access, you will be able to download patches (required updates) and then transmit them to isolated Administration Servers.

> You can download the third-party software updates issued by software vendors, but you cannot download updates for Microsoft software on isolated Administration Servers by using Kaspersky Security Center.

For more details about the process of fixing vulnerabilities in an isolated network, see the description and scheme of this process.

## Prerequisites

Before you start, do the following:

1. Allocate one device for connecting to the internet and downloading patches. This device will be considered the Administration Server with internet access.
2. Install Kaspersky Security Center Linux, no earlier than version 15.1, on the following devices:
   - Allocated device, which will act as the Administration Server with internet access
   - Isolated devices, which will act as the Administration Servers isolated from the internet (hereinafter referred to as isolated Administration Servers)
3. Make sure that every Administration Server has enough disk space for downloading and storing updates and patches.

## Stages

Installing updates and fixing third-party software vulnerabilities on the managed devices of isolated Administration Servers consists of the following stages:

1. **Configuring the Administration Server with internet access**

   Prepare your Administration Server with internet access to handle requests for required third-party software updates and to download patches.

2. **Configuring isolated Administration Servers**

   Prepare your isolated Administration Servers so they can regularly form lists of required updates and handle patches downloaded by the Administration Server with internet access. After configuring, isolated Administration Servers do not try to download patches from the internet anymore. Instead, they get updates through patches.

3. **Transmitting patches and installing updates on isolated Administration Servers**

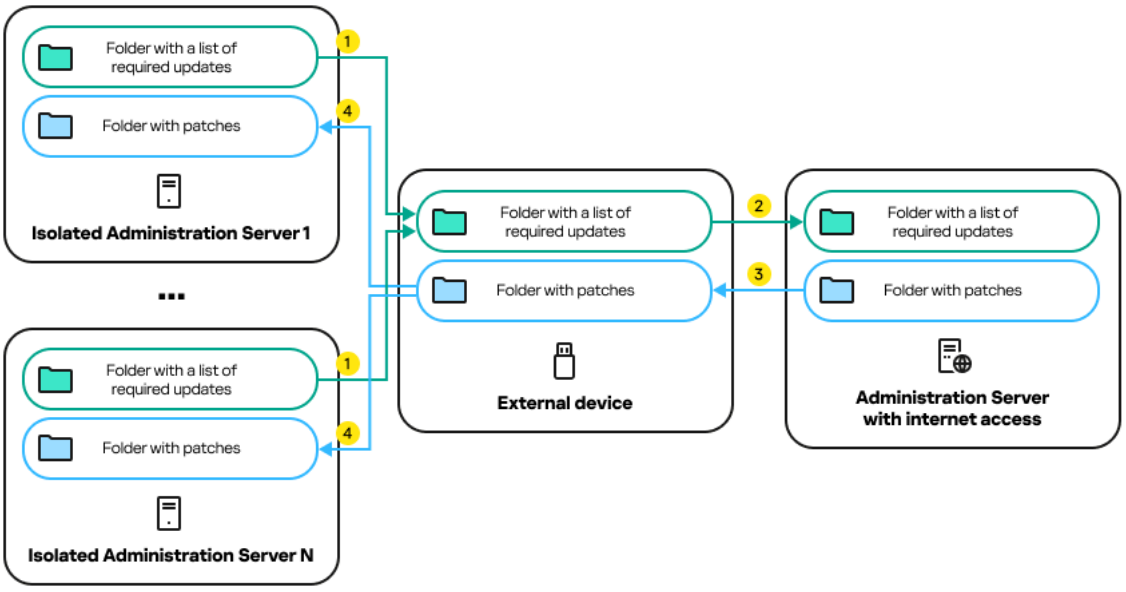
   After you finish configuring Administration Servers, you can transmit the required update lists and patches from the Administration Server with internet access to isolated Administration Servers. Next, updates from patches will be installed on managed devices by using the *Install required updates and fix vulnerabilities* task.

## Results

Thus, the third-party software updates are transmitted to isolated Administration Servers and installed on connected managed devices by using Kaspersky Security Center Linux. It is enough to configure Administration Servers once, and after that, you can get updates as often as you need, for example, once or several times per day.

# About fixing third-party software vulnerabilities in an isolated network

The process of fixing third-party software vulnerabilities in an isolated network is shown in the figure below. You can repeat this process periodically.




The process of transmitting patches and the list of required updates between the Administration Server with internet access and isolated Administration Servers

Every Administration Server isolated from the internet (hereinafter referred to as an isolated Administration Server) generates a list of updates that must be installed on managed devices connected to this Administration Server. This list of updates is stored in a specific folder as a set of binary files, each named with the ID of the patch containing the necessary update. Therefore, each file in the list corresponds to a specific patch.

The list of required updates is transferred from the isolated Administration Server to the designated Administration Server with internet access by using an external device. After that, the designated Administration Server downloads patches from the internet and places them in a designated folder.

When all patches are downloaded and placed in the designated folder, they are then transferred back to each isolated Administration Server from which the list of required updates was obtained. The patches are saved in a folder specifically created for them on each isolated Administration Server.

As a result, the *Install required updates and fix vulnerabilities* task runs patches and installs updates on managed devices of the isolated Administration Servers.

# Configuring the Administration Server with internet access to fix vulnerabilities in an isolated network

To prepare for fixing vulnerabilities and transmitting patches within an isolated network, the initial step is to configure an Administration Server with internet access, and then to configure isolated Administration Servers.

*To configure an Administration Server with internet access:*

1. Create two folders on the disk where the Administration Server is installed:

   - Folder for the list of required updates
   - Folder for patches

   You can give these folders any name you want.

2. Grant the **Modify** right to the KLAdmins group in the created folders, by using the standard administrative tools of the operating system.

3. Use the klscflag utility to specify the paths to the folders in the Administration Server properties.

   Run the command line, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.

4. Run the following commands in the command line:

   - To set the path to the folder for patches:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<path to the folder>"`
   - To set the path to the folder for the list of required updates:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<path to the folder>"`

   Example: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/FolderForPatches"`

5. If necessary, use the klscflag utility to specify how often the Administration Server should check for new patch requests:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <value in seconds>`

   The default setting is 120 seconds.

   Example: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. Create the *Find vulnerabilities and required updates* task to obtain information about patches for the third-party software installed on the managed devices, and then set the task schedule.

7. Create the *Fix vulnerabilities* task to specify patches for the third-party software used to fix vulnerabilities, and then set the task schedule.

   Run tasks manually if you want them to run earlier than it is specified in the schedule. The order in which tasks are started is important. The *Fix vulnerabilities* task must be run after finishing the *Find vulnerabilities and required updates* task.

8. Restart the Administration Server service.

The Administration Server with internet access is ready to download and transmit updates to isolated Administration Servers. Before you start fixing vulnerabilities, configure the isolated Administration Servers.

# Configuring isolated Administration Servers to fix vulnerabilities in an isolated network

After configuring the Administration Server with internet access, prepare every isolated Administration Server within your network to fix vulnerabilities and install updates on managed devices connected to these isolated Administration Servers.

*To configure isolated Administration Servers, follow the steps below for each Administration Server:*

1. Activate a license key for the Vulnerability and patch management (VAPM) feature.
2. Create two folders on the disk where the Administration Server is installed:
   - Folder for the list of required updates
   - Folder for patches

   You can give these folders any name you want.
3. Grant the **Modify** right to the KLAdmins group in the created folders, by using the standard administrative tools of the operating system.
4. Use the klscflag utility to specify the paths to the folders in the Administration Server properties.

   Run the command line, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.
5. Run the following commands in the command line:
   - To set the path to the folder for patches:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<path to the folder>"
     ```
   - To set the path to the folder for the list of required updates:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<path to the folder>"
     ```

   Example: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`
6. If necessary, use the klscflag utility to specify how often the isolated Administration Server should check for new patches:
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <value in seconds>
   ```
   The default setting is 120 seconds.

   Example: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`
7. If necessary, use the klscflag utility to calculate the SHA256 hashes of patches:
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
   ```
   By running this command, you can make sure that the patches have not been modified during their transfer to the isolated Administration Server and that you have received the correct patches containing the required updates.

By default, Kaspersky Security Center Linux does not calculate the SHA256 hashes of patches. If you enable this option, after the isolated Administration Server receives patches, Kaspersky Security Center Linux computes their hashes and compares the acquired values with the hashes stored in the Administration Server database. If the calculated hash does not match the hash in the database, an error occurs and you have to replace the incorrect patches.

8. Create the *Find vulnerabilities and required updates* task to obtain information about patches for the third-party software installed on the managed devices, and then set the task schedule.

9. Create the *Fix vulnerabilities* task to specify patches for the third-party software used to fix vulnerabilities, and then set the task schedule.

   Run tasks manually if you want them to run earlier than it is specified in the schedule. The order in which tasks are started is important. The *Fix vulnerabilities* task must be run after finishing the *Find vulnerabilities and required updates* task.

10. Restart the Administration Server service.

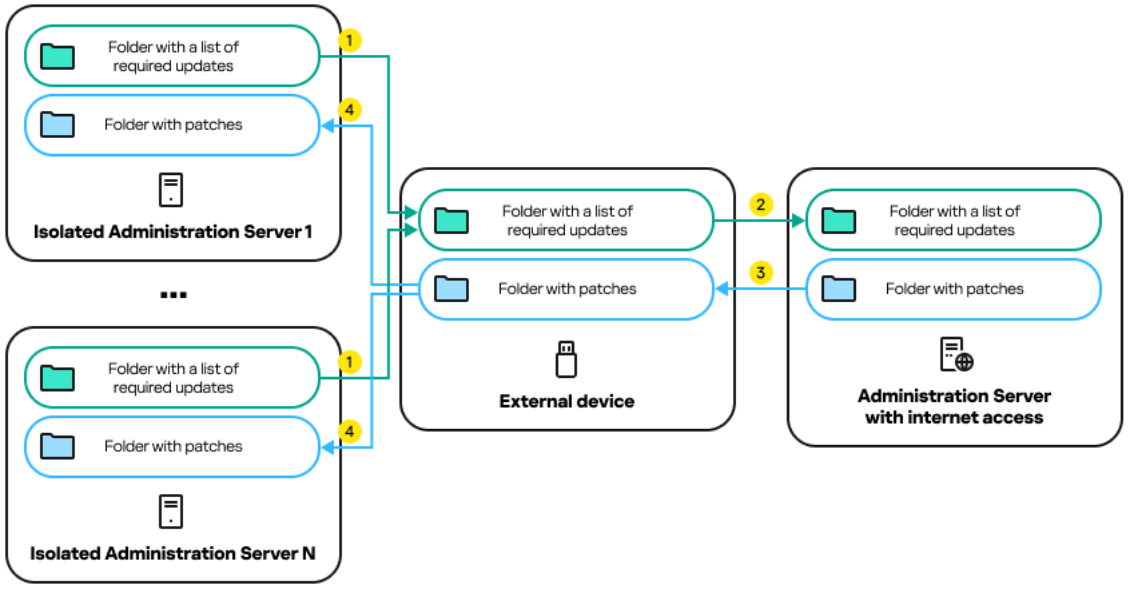
After configuring all Administration Servers, you can transmit patches and lists of required updates and fix third-party software vulnerabilities on managed devices within the isolated network.

# Transmitting patches and installing updates in an isolated network

After you have finished configuring Administration Servers, you can transfer patches containing the required updates from the Administration Server with internet access to isolated Administration Servers. You can transmit and install updates as often as you need, for example, once or several times per day.

You need an external device, such as a removable drive, to transfer patches and the list of required updates between Administration Servers. Therefore, make sure that the external device has enough disk space for downloading and storing patches.

The process of transmitting patches and the list of required updates are shown in the figure below:




The process of transmitting patches and the list of required updates between the Administration Server with internet access and isolated Administration Servers

*To install updates and fix vulnerabilities on managed devices connected to isolated Administration Servers:*

1. Start the *Install required updates and fix vulnerabilities* task if it is not yet running.
2. Connect an external device to any isolated Administration Server.
3. Create two folders on the external device: one for the list of required updates and one for patches. You can give these folders any name you want.

   If you created these folders earlier, clear them.
4. Copy the list of required updates from every isolated Administration Server and paste this list into the folder for the list of required updates on the external device.

   As a result, you unite all lists acquired from all isolated Administration Servers into one folder. This folder contains binary files with the IDs of patches required for all isolated Administration Servers.
5. Connect the external device to the Administration Server with internet access.
6. Copy the list of required updates from the external device and paste this list into the folder for the list of required updates on the Administration Server with internet access.

   All required patches are automatically downloaded from the internet to the folder for patches on the Administration Server. This can take several hours.
7. Make sure that all required patches are downloaded. For this purpose, you can do one of the following:

   - Check the folder for patches on the Administration Server with internet access. All patches that were specified in the list of required updates should be downloaded to the necessary folder. This is more convenient if a small number of patches are required.
   - Prepare a special script, for example, a shell script. If you get a large number of patches, this will be difficult to check on your own that all patches have been downloaded. In such cases, it is better to automate the check.
8. Copy the patches from the Administration Server with internet access and paste them into the corresponding folder on your external device.
9. Transfer the patches to every isolated Administration Server. Put the patches into a specific folder for them.

As a result, every isolated Administration Server creates an actual list of updates that are required for managed devices connected to the current Administration Server. After the Administration Server with internet access receives the list of required updates, the Administration Server downloads patches from the internet. When these patches appear on isolated Administration Servers, the *Install required updates and fix vulnerabilities* task handles the patches. Thus, updates are installed on managed devices, and third-party software vulnerabilities are fixed.

When the *Install required updates and fix vulnerabilities* task is running, do not reboot the Administration Server device and do not run the *Backup of Administration Server data* task (it will also cause a reboot). As a result, the *Install required updates and fix vulnerabilities* task is interrupted, and updates are not installed. In this case, you have to restart this task manually or wait for the task to start according to the configured schedule.

# Disabling transmission of patches and installation of updates in an isolated network

You can disable the transmission of patches to isolated Administration Servers, for example, if you decide to take one or more Administration Servers out of an isolated network. Thus, you can reduce the number of patches and the time to download them.

*To disable transmission of patches to isolated Administration Servers:*

1. If you want to remove all Administration Servers from isolation, in the properties of the Administration Server with internet access, delete the paths to the folders intended for patches and the list of required updates. If you want to keep specific Administration Servers within an isolated network, skip this step.

   Run the command line, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.

   Run the following commands in the command line:

   - To delete the path to the folder for patches:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - To delete the path to the folder for the list of required updates:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```
2. Restart service on the Administration Server with internet access if you deleted the paths to the folders.
3. In the properties of each isolated Administration Server that you want to remove from the isolated network, delete the paths to the folders for patches and the list of required updates.

   Run the following commands in the command line under an account with root privileges:

   - To delete the path to the folder for patches:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - To delete the path to the folder for the list of required updates:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```
4. Restart the service of each Administration Server on which you deleted the paths to the folders.

If you reconfigured the Administration Server with internet access, patches will no longer be transmitted via Kaspersky Security Center Linux.

If you reconfigured only specific Administration Servers and removed them from the isolated network, they will no longer receive patches via Kaspersky Security Center Linux. Only those Administration Servers that remain within the isolated network will continue to receive patches.

If you want to start fixing vulnerabilities on disabled isolated Administration Servers in the future, you have to configure these Administration Servers and the Administration Server with internet access once again.

# API Reference Guide

This Kaspersky Security Center OpenAPI reference guide is designed to assist in the following tasks:

- Automation and customization. You can automate tasks that you might not want to handle manually. For example, as an administrator, you can use Kaspersky Security Center OpenAPI to create and run scripts that will facilitate developing the structure of administration groups and keep that structure up-to-date.
- Custom development. Using OpenAPI, you can develop a client application.

You can use the search field in the right part of the screen to locate the information you need in the OpenAPI reference guide.

OpenAPI Reference Guide

## Samples of scripts

The OpenAPI reference guide contains samples of the Python scripts listed in the table below. The examples show how you can call OpenAPI methods and automatically perform various tasks for protecting your network, for instance, create a "primary/secondary" hierarchy, run tasks in Kaspersky Security Center Linux, or assign distribution points. You can run the samples as is or create your own scripts based on the samples.

*To call the OpenAPI methods and run scripts,*

Install the KlAkOAPI package from the KlAkOAPI.tar.gz archive on a device where Administration Server is installed.

The KlAkOAPI package includes a set of samples that perform typical operations. You can call the OpenAPI methods, run the samples and your own scripts only on devices where Administration Server and the KlAkOAPI package are installed. The KlAkOAPI.tar.gz archive that contains this package is located in the Kaspersky Security Center Linux installation folder.

Matching between user scenarios and samples of Kaspersky Security Center OpenAPI methods

| Example | Purpose of the sample | Scenario |
|---|---|---|
| Log KlAkParams | You can extract and process data by using the `KlAkParams` data structure. The sample shows how to work with this data structure.<br>The sample output may be present in different ways. You can get the data to send an HTTP method or to use it in your code. | Monitoring and reporting |
| Create and delete a "primary/secondary" hierarchy | You can add a secondary Administration Server and establish a "primary/secondary" hierarchy. Alternately, you can disconnect the secondary Administration Server from the hierarchy. | Creating a hierarchy of Administration Servers, adding a secondary Administration Server, and deleting a hierarchy of Administration Servers |
| Download network list files via connection gateway to the specified host | You can connect to Network Agent on the needed device by using a connection gateway, and then download a file with the network list to your device. | Adjustment of distribution points and connection gateways |
| Install a license key stored in the primary Administration Server repository onto the secondary Administration Servers | You can connect to the primary Administration Server, download a required license key from it, and transmit this key to all the secondary Administration Servers included in a hierarchy. | Licensing of managed applications |

| Example | Purpose of the sample | Scenario |
| --- | --- | --- |
| Create a report of effective user rights | You can create different reports. For instance, you can generate the report of effective user rights by using this sample. This report describes the rights that a user has, depending on his or her group and role.<br>You can download the report in the HTML, PDF, or Excel format. | Generating and viewing a report |
| Start the device task | You can connect to Network Agent on the needed device by using a connection gateway, and then run the necessary task. | Starting a task manually |
| Register distribution points for devices in a group | You can assign managed devices as distribution points (previously known as update agents). | Updating Kaspersky databases and applications |
| Enumerate all groups | You can perform various actions with administration groups. The sample shows how to do the following:<br>• Get an identifier of the "Managed devices" root group<br>• Move through the group hierarchy<br>• Retrieve the full, expanded hierarchy of groups, along with their names and nesting | Configuring Administration Server |
| Enumerate tasks, query task statistics, and run a task | You can find out the following information:<br>• Task progress history<br>• Current task status<br>• Number of tasks in different statuses<br>You can also run a task. By default, the sample runs a task after it outputs statistics. | Managing tasks |
| Create and run a task | You can create a task. Specify the following task parameters in the sample:<br>• Type<br>• Method of run<br>• Name<br>• Device group for which the task will be used<br>By default, the sample creates a task with the "Show message" type. You can run this task for all managed devices of Administration Server. If necessary, you can specify your own task parameters. | Creating a task |
| Enumerate license keys | You can get a list of all the active license keys for Kaspersky applications installed on managed devices of Administration Server. The list contains detailed data about every license key, such as a name, type, or expiration date. | Viewing information about license keys in use |
| Create and find an internal user | You can create an account for further work. | Adding an account of an internal user |
| Create a custom category | You can create the application category with the needed parameters. | Creating an application category with content added manually |
| Enumerate users by using SrvView | You can use the SrvView class to request detailed information from the Administration Server. For instance, you can get a list of users by using this sample. | Managing users and user roles |
| Create internal users, create and email an Android installation package | You can create internal users by using the SecurityPolicy class, create an Android installation package, and send it to the users by email. | Adding an account of an internal user |

## Applications interacting with Kaspersky Security Center Linux via OpenAPI

Some applications interact with Kaspersky Security Center Linux via OpenAPI. These applications include, for example, Kaspersky Anti Targeted Attack Platform or Kaspersky Security for Virtualization. It can also be a custom client application that you can develop using OpenAPI.

Applications interacting with Kaspersky Security Center Linux via OpenAPI connect to Administration Server. If you have configured an allowlist of IP addresses for connecting to the Administration Server, add IP addresses of devices where applications using Kaspersky Security Center Linux OpenAPI are installed. To find out whether the application that you use works by OpenAPI, see Help of this application.

# Best Practices for Service Providers

This section provides information about how to configure and use Kaspersky Security Center Linux.

This section contains recommendations on how to deploy, configure, and use the application, as well as describes ways of resolving typical issues in the application operation.

# Planning Kaspersky Security Center Linux deployment

When planning the deployment of Kaspersky Security Center Linux components on an organization's network, you must take into account the size and scope of the project; specifically, the following factors:

- Total number of devices
- Number of MSP clients

One Administration Server can support a maximum of 50,000 devices. If the total number of devices on an organization's network exceeds 50,000, multiple Administration Servers must be deployed on the service provider side and combined into a hierarchy for convenient centralized management.

Up to 500 virtual Servers can be created on a single Administration Server, so an individual Administration Server is required for each 500 MSP clients.

At the stage of deployment planning, the assignment of the special certificate X.509 to the Administration Server must be considered. Assignment of the X.509 certificate to the Administration Server may be useful in the following cases (partial list):

- Inspecting secure socket layer (SSL) traffic by means of an SSL termination proxy
- Specifying required values in certificate fields
- Providing the required encryption strength of a certificate

# Providing internet access to Administration Server

To allow devices on the client network to access Administration Server over the internet, you have to make available the following Administration Server ports:

- 13000 TCP—Administration Server TLS port for connecting Network Agents deployed on the client network
- 8061 TCP—HTTPS port for publishing stand-alone packages using Kaspersky Security Center Web Console tools
- 8060 TCP—HTTP port for publishing stand-alone packages using Kaspersky Security Center Web Console tools

- 13292 TCP—TLS port required only if there are mobile devices that need to be managed
- 8080 TCP—HTTPS port for Kaspersky Security Center Web Console

# Kaspersky Security Center Linux standard configuration

One or several Administration Servers are deployed on the MSPs' servers. The number of Administration Servers can be selected either based on available hardware, or on the total number of MSP clients served or total number of managed devices.

One Administration Server can support up to 50,000 devices. You must consider the possibility of increasing the number of managed devices in the near future: it may be useful to connect a slightly smaller number of devices to a single Administration Server.

Up to 500 virtual Servers can be created on a single Administration Server, so an individual Administration Server is required for each 500 MSP clients.

If multiple Servers are used, it is recommended that you combine them into a hierarchy. Using a hierarchy of Administration Servers allows you to avoid dubbed policies and tasks, handle the whole set of managed devices, as if they are managed by a single Administration Server: i.e., search for devices, build selections of devices, and create reports.

On each virtual Server that corresponds to an MSP client, you must assign one or several distribution point(s). If MSP clients and the Administration Server are linked through the internet, it may be useful to create a *Download updates to the repositories of distribution points* task for the distribution points, so that they will download updates directly from Kaspersky servers, not from the Administration Server.

If some devices in the MSP client network have no direct internet access, you have to switch the distribution points to the connection gateway mode. In this case, Network Agents on devices on the MSP client network will be connected, for further synchronization, to the Administration Server—but through the gateway, not directly.

As the Administration Server, most probably, will not be able to poll the MSP client network, it may be useful to turn this function over to a distribution point.

The Administration Server will not be able to send notifications to port 15000 UDP to managed devices located behind the NAT on the MSP client network. To resolve this issue, it may be useful to enable the mode of continuous connection to the Administration Server in the properties of devices acting as distribution points and running in connection gateway mode (**Do not disconnect from the Administration Server** option). The continuous connection mode is available if the total number of distribution points does not exceed 300.

An MSP client might want to manage Android and iOS devices of the employees. Administration Server manages mobile devices through TLS, TCP port 13292.

# About distribution points

A device with Network Agent installed can be used as a distribution point. In this mode, Network Agent can perform the following functions:

- Transfer files to client devices, including:
  - Updates of Kaspersky databases and software modules

    Updates can be received either from the Administration Server or from Kaspersky update servers. In the latter case, the *Download updates to the repositories of distribution points* task must be created for the device serving as the distribution point.
  - Third-party software updates
  - Installation packages
- Install software (including initial deployment of Network Agents) on other devices.
- Poll the network to detect new devices and update information about existing ones. A distribution point can apply the same device discovery methods as the Administration Server.

Deployment of distribution points on an organization's network has the following objectives:

- Reduce the load on the Administration Server if it functions as the update source.
- Optimize internet traffic since, in this case, each device on the MSP client network does not have to access Kaspersky servers or the Administration Server for updates.
- Provide the Administration Server access to devices behind the NAT (relative to the Administration Server) of the MSP client network, which allows the Administration Server to perform the following actions:
  - Send notifications to devices over UDP on the IPv4 or IPv6 network
  - Poll the IPv4 or IPv6 network
  - Perform initial deployment
  - Act as a push server

A distribution point is assigned for an administration group. In this case, the scope of the distribution point includes all devices within the administration group and all of its subgroups. However, the device acting as the distribution point does not have to be included in the administration group to which it has been assigned.

You can make a distribution point function as a connection gateway. In this case, devices in the scope of this distribution point will be connected to the Administration Server through the gateway, not directly. You can use this mode in scenarios that do not allow the establishment of a direct connection between devices with Network Agent and an Administration Server.

Devices functioning as distribution points must be protected, including physical protection, against any unauthorized access.

# Hierarchy of Administration Servers

Some client companies, for example MSP, may run multiple Administration Servers. It can be inconvenient to administer several separate Administration Servers, so a hierarchy can be applied. In a hierarchy, a Linux-based Administration Server can work both as a primary Server and as a secondary Server. The primary Linux-based Server can manage both Linux-based and Windows-based secondary Servers. A primary Windows-based Server can manage a secondary Linux-based Server.

A "primary/secondary" configuration for two Administration Servers provides the following options:

- A secondary Administration Server inherits policies, tasks, user roles, and installation packages from the primary Administration Server, thus preventing duplication of settings.
- Selections of devices on the primary Administration Server can include devices from secondary Administration Servers.
- Reports on the primary Administration Server can contain data (including detailed information) from secondary Administration Servers.
- A primary Administration Server can be used as a source of updates for a secondary Administration Server.

The primary Administration Server only receives data from non-virtual secondary Administration Servers within the scope of the options listed above. This limitation does not apply to virtual Administration Servers, which share the database with their primary Administration Server.

Hierarchy of Administration Servers provides support for multitenancy mode. This mode allows a main administrator to centrally manage multiple clients independently. Each client organization or office is isolated from others and is referred to as a tenant. You can allocate multiple managed devices along with their associated data, settings, policies, and tasks to a tenant, and configure user rights by tenant.

A primary Administration Server, installed in the main organization infrastructure, acts as a primary tenant. The primary Administration Server enables secondary or virtual Administration Servers—its isolated tenants—to independently receive and process their own events and work with their own resources, services, and configurations.

A service provider that has a number of client organizations can provide the Kaspersky Security Center Linux functionality, including alert aggregation and response actions, to each client organization independently. To achieve this, the service provider connects secondary or virtual Administration Servers as tenants for each client organization. The service provider delivers services by using their own personnel and resources.

# Virtual Administration Servers

On the basis of a physical Administration Server, multiple virtual Administration Servers can be created, which will be similar to secondary Administration Servers. Compared to the discretionary access model, which is based on access control lists (ACLs), the virtual Administration Server model is more functional and provides a larger degree of isolation. In addition to a dedicated structure of administration groups for assigned devices with policies and tasks, each virtual Administration Server features its own group of unassigned devices, own sets of reports, selected devices and events, installation packages, moving rules, etc. For maximum mutual isolation of MSP clients, we recommend that you choose virtual Administration Servers as the functionality to be used. In addition, creating a virtual Administration Server for each MSP client allows you to provide clients basic options of network administration through Kaspersky Security Center Web Console.

Virtual Administration Servers are very similar to secondary Administration Servers, but with the following distinctions:

- A virtual Administration Server lacks most global settings and its own TCP ports.
- A virtual Administration Server has no secondary Administration Servers.
- A virtual Administration Server has no other virtual Administration Servers.
- A physical Administration Server views devices, groups, events, and objects on managed devices (items in Quarantine, applications registry, etc.) of all its virtual Administration Servers.
- A virtual Administration Server can only scan the network with distribution points connected.

# Deployment and initial configuration

Kaspersky Security Center Linux is a distributed application. Kaspersky Security Center Linux includes the following applications:

- Administration Server—The core component, designed for managing devices of an organization and storing data in a DBMS.
- Kaspersky Security Center Web Console—A web interface for Administration Server designed for basic operations. You can install this component on any device that meets the hardware and software requirements.
- Network Agent—Designed for managing the security application installed on a device, as well as getting information about that device. Network Agents are installed on devices of an organization.

Deployment of Kaspersky Security Center Linux on an organization's network is performed as follows:

- Installation of Administration Server
- Installation of Kaspersky Security Center Web Console
- Installation of Network Agent and the security application on devices of the enterprise

# Recommendations on Administration Server installation

This section contains recommendations on how to install Administration Server. This section also provides scenarios for using a shared folder on the Administration Server device in order to deploy Network Agent on client devices.

## Creating accounts for the Administration Server services on a failover cluster

Before you start deployment of Kaspersky Security Center Linux on a failover cluster, you must create accounts for Kaspersky Security Center Linux services.

To do this, perform the following steps on the active node, passive node, and the file server:

1. Create a group with the name 'kladmins' and assign the same GID to all three groups.
2. Create a user account with the name 'ksc' and assign the same UID to all three user accounts. Set the primary group to 'kladmins' for the created accounts.
3. Create a user account with the name 'rightless' and assign the same UID to all three user accounts. Set the primary group to 'kladmins' for the created accounts.

## Selecting a DBMS

The following table lists the valid DBMS options, as well as the recommendations and restrictions on their use.

Recommendations and restrictions on DBMS

| DBMS | Recommendations and limitations |
|---|---|
| MySQL (see supported versions) | Use this DBMS if you intend to run a single Administration Server for less than 20,000 devices. |
| MariaDB (see supported versions) | Use this DBMS if you intend to run a single Administration Server for less than 20,000 devices. |
| PostgreSQL, Postgres Pro (see supported versions) | Use this DBMS if you intend to run a single Administration Server for less than 50,000 devices. |
| Tantor (see supported versions) | Use this DBMS if you intend to run a single Administration Server for less than 50,000 devices.<br>The Tantor DBMS is only supported on Astra Linux Special Edition RUSB.10015-01 (operational update 1.8). |

For information about how to install the selected DBMS, refer to its documentation.

It is recommended to disable the Software inventory task and disable (in the Kaspersky Endpoint Security policy settings) notifications of Administration Server on started applications.

If you decide to install PostgreSQL or Postgres Pro DBMS, ensure that you specified a password for the superuser. If the password is not specified, Administration Server might not be able to connect to the database.

If you install MySQL, MariaDB, PostgreSQL, or Postgres Pro, use the recommended settings to ensure the DBMS functions properly.

If you use a PostgreSQL, MariaDB or MySQL DBMS, the **Events** tab may display an incomplete list of events for the selected client device. This occurs when the DBMS stores a very large amount of events. You can increase the number of displayed events by doing either of the following:

- Removing unnecessary events.
- Reducing the storage term for unnecessary events.

To see a full list of events logged on the Administration Server for the device, use Reports.

## Specifying the address of the Administration Server

When installing Administration Server, you must specify the DNS name or static IP address of the Administration Server. This address will be used as the default address when creating installation packages of Network Agent. After that, you will be able to change the address of the Administration Server host by using Kaspersky Security Center Web Console tools; the address will not change automatically in Network Agent installation packages that have been already created.

## Maintaining idle connections

We recommend that you configure the following keepalive parameters on connection gateway devices to improve connection stability:

- `net.ipv4.tcp_keepalive_intvl` specifies how often to send keepalive messages after the first one. Set this parameter to `1`.
- `net.ipv4.tcp_keepalive_probes` specifies how many keepalive messages can be sent without a reply before the connection is considered dead. Set this parameter to `10`.
- `net.ipv4.tcp_keepalive_time` specifies how long to wait after the last data packet before sending the first keepalive message. Set this parameter to `900`.

*To configure keepalive parameters:*

1. Open the /etc/sysctl.conf file.
2. Add the following parameter values:

```
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_probes = 10
net.ipv4.tcp_keepalive_time = 900
```

3. Run the following command to update keepalive parameters:

```
sudo sysctl -p /etc/sysctl.conf
```

4. Run the following commands to ensure that parameter values have been applied:

```
sudo sysctl net.ipv4.tcp_keepalive_intvl
sudo sysctl net.ipv4.tcp_keepalive_probes
sudo sysctl net.ipv4.tcp_keepalive_time
```

# Deploying Network Agent and security applications

To manage devices in an organization and to protect them against security threats, you have to install Network Agent and a Kaspersky security application on each of them.

For information about protection deployment, refer to the Deploying Network Agent and the security application section.

For information about mobile device protection, refer to the Mobile Device Management section.

In Microsoft Windows XP, Network Agent might not perform the following operations correctly: downloading updates directly from Kaspersky servers (as a distribution point) and functioning as a KSN proxy server (as a distribution point); and detecting third-party vulnerabilities (if Vulnerability and patch management is used).

# Configuring protection on a client organization's network

After Administration Server installation is complete, Kaspersky Security Center Web Console launches and prompts you to perform the initial setup through the relevant wizard. When the quick start wizard is running, the following policies and tasks are created in the root administration group:

- Policy of Kaspersky Endpoint Security
- Group task for updating Kaspersky Endpoint Security
- Group task for scanning a device with Kaspersky Endpoint Security
- Policy of Network Agent
- Vulnerability scan task (task of Network Agent)
- Updates installation and vulnerabilities fix task (task of Network Agent)

Policies and tasks are created with the default settings, which may turn out to be sub-optimal or even inadmissible for the organization. Therefore, you must check the properties of objects that have been created and modify them manually, if necessary.

This section contains information about manual configuration of policies, tasks, and other settings of Administration Server, and information about the distribution point, building an administration group structure and hierarchy of tasks, and other settings.

## Manual setup of the Kaspersky Endpoint Security policy

This section provides recommendations on how to configure the Kaspersky Endpoint Security policy, which is created by the quick start wizard. You can perform setup in the policy properties window.

When editing a setting, keep in mind that you can lock or unlock the setting in order to prohibit or allow editing its value on a workstation.

## Configuring the policy in the Advanced Threat Protection section

For a full description of the settings in this section, please refer to the Kaspersky Endpoint Security for Windows documentation.

In the **Advanced Threat Protection** section, you can configure the use of Kaspersky Security Network for Kaspersky Endpoint Security for Windows. You can also configure Kaspersky Endpoint Security for Windows modules, such as Behavior Detection, Exploit Prevention, Host Intrusion Prevention, and Remediation Engine.

In the **Kaspersky Security Network** subsection, we recommend that you enable the **Kaspersky Security Network** option. Using this option helps to redistribute and optimize traffic on the network. If the **Kaspersky Security Network** option is disabled, you can enable direct use of KSN servers.

## Configuring the policy in the Essential Threat Protection section

For a full description of the settings in this section, please refer to the Kaspersky Endpoint Security for Windows documentation.

In the **Essential Threat Protection** section of the policy properties window, we recommend that you specify additional settings in the **Firewall** and **File Threat Protection** subsections.

The **Firewall** subsection contains settings that allow you to control the network activity of applications on the client devices. A client device uses a network to which one of the following statuses is assigned: public, local, or trusted. Depending on the network status, Kaspersky Endpoint Security can allow or deny network activity on a device. When you add a new network to your organization, you must assign an appropriate network status to it. For example, if the client device is a laptop, we recommend that this device use the public or trusted network, because the laptop is not always connected to the local network. In the **Firewall** subsection, you can check whether you correctly assigned statuses to the networks used in your organization.

*To check the list of networks:*

1. In the policy properties, go to **Essential Threat Protection** → **Firewall**.
2. In the **Available networks** section, click the **Settings** button.
3. In the **Firewall** window that opens, go to the **Networks** tab to view the list of networks.

In the **File Threat Protection** subsection, you can disable the scanning of network drives. Scanning network drives can place a significant load on network drives. It is more convenient to perform indirect scanning on file servers.

*To disable scanning of network drives:*

1. In the policy properties, go to **Essential Threat Protection** → **File Threat Protection**.
2. In the **Security level** section, click the **Settings** button.
3. In the **File Threat Protection** window that opens, on the **General** tab clear the **All network drives** check box.

## Configuring the policy in the General Settings section

For the full description of the settings in this section, please refer to the Kaspersky Endpoint Security documentation.

Described below are advanced setup actions, which we recommend that you perform in the policy properties window of Kaspersky Endpoint Security, in the **General Settings** section.

General Settings section, Reports and Storage subsection

In the **Data transfer to Administration Server** section, please note the **About started applications** check box. If this check box is selected, the Administration Server database saves information about all versions of all software modules on the networked devices. This information may require a significant amount of disk space in the Kaspersky Security Center Linux database (dozens of gigabytes). Therefore, if the **About started applications** check box is still selected in the top-level policy, it must be cleared.

General Settings section, Interface subsection

If the threat protection in the organization's network must be managed in centralized mode through Kaspersky Security Center Web Console, you must disable the display of the Kaspersky Endpoint Security user interface on workstations (by clearing the **Display application interface** check box in the **Interaction with user** section), and enable password protection (by selecting the **Enable password protection** check box in the **Password protection** section).

## Configuring the policy in the Event configuration section

In the **Event configuration** section, you should disable the saving of any events on Administration Server, except for the following ones:

- On the **Critical** tab:
  - *Application autorun is disabled*
  - *Access denied*
  - *Application startup prohibited*
  - *Disinfection impossible*
  - *End User License Agreement violated*
  - *Could not load encryption module*
  - *Cannot start two tasks at the same time*
  - *Active threat detected. Advanced Disinfection should be started*
  - *Network attack detected*
  - *Not all components were updated*

- *Activation error*
- *Error enabling portable mode*
- *Error in interaction with Kaspersky Security Center*
- *Error disabling portable mode*
- *Error changing application components*
- *Error applying file encryption / decryption rules*
- *Policy cannot be applied*
- *Process terminated*
- *Network activity blocked*

- On the **Functional failure** tab: *Invalid task settings. Settings not applied*
- On the **Warning** tab:
  - *Self-Defense is disabled*
  - *Incorrect reserve key*
  - *User has opted out of the encryption policy*
- On the **Info** tab: *Application startup prohibited in test mode*

## Manual setup of the group update task for Kaspersky Endpoint Security

If the Administration Server acts as the update source, the optimal and recommended schedule option for Kaspersky Endpoint Security is **When new updates are downloaded to the repository** with the **Use automatically randomized delay for task starts** check box selected.

If a local task for downloading updates from Kaspersky servers to the repository is created on each distribution point, periodic scheduling will be optimal and recommended for the Kaspersky Endpoint Security group update task. In this case, the randomization interval value should be set on 1 hour.

## Manual setup of the group task for scanning a device with Kaspersky Endpoint Security

The quick start wizard creates a group task for scanning a device. If the automatically specified schedule of the group scanning task is not appropriate for your organization, you must manually set up the most convenient schedule for this task based on the workplace rules adopted in the organization.

For example, the task is assigned a **Run on Fridays at 7:00 PM** schedule with automatic randomization, and the **Run missed tasks** check box is cleared. This means that if the devices in the organization are shut down on Fridays, for example, at 6:30 PM, the device scan task will never run. In this case you need to set up the group scanning task manually.

## Scheduling the Find vulnerabilities and required updates task

The quick start wizard creates the *Find vulnerabilities and required updates* task for Network Agent. By default, the task is assigned a **Run on Tuesdays at 7:00 PM** schedule with automatic randomization, and the **Run missed tasks** check box is selected.

If the organization's workplace rules provide for shutting down all devices at this time, the *Find vulnerabilities and required updates task* will run after the devices are turned on again, that is, on Wednesday morning. Such activity may be undesirable because a vulnerability scan may increase the load on CPUs and disk subsystems. You must set up the most convenient schedule for the task based on the workplace rules adopted in the organization.

## Manual setup of the group task for updates installation and vulnerabilities fix

The quick start wizard creates a group task for updates installation and vulnerabilities fix for Network Agent. By default, the task is set up to run every day at 01:00 AM, with automatic randomization, and the **Run missed tasks** option is not enabled.

If the organization's workplace rules provide for shutting down devices overnight, the update installation will never run. You must set up the most convenient schedule for the vulnerability scan task based on the workplace rules adopted in the organization. It is also important to keep in mind that installation of updates may require restarting the device.

## Building a structure of administration groups and assigning distribution points

A structure of administration groups in Kaspersky Security Center Linux performs the following functions:

- Sets the scope of policies

  There is an alternate way of applying relevant settings on devices, by using policy profiles. In this case, the scope of policies is set, for example, with device tags or user roles.

- Sets the scope of group tasks

  There is an approach to defining the scope of group tasks that is not based on a hierarchy of administration groups: use of tasks for device selections and tasks for specific devices.

- Sets access rights to devices, virtual Administration Servers, and secondary Administration Servers

- Assigns distribution points

When building the structure of administration groups, you must take into account the topology of the organization's network for the optimum assignment of distribution points. The optimum distribution of distribution points allows you to save traffic on the organization's network.

Depending on the organizational schema and network topology adopted by the MSP client, the following standard configurations can be applied to the structure of administration groups:

- Single office
- Multiple small remote offices

## Standard MSP client configuration: Single office

In a standard "single-office" configuration, all devices are on the organization's network so they can "see" each other. The organization's network may consist of a few separate parts (networks or network segments) linked by narrow channels.

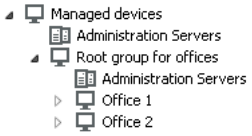
The following methods of building the structure of administration groups are possible:

- Building the structure of administration groups taking into account the network topology. The structure of administration groups may not reflect the network topology with absolute precision. A match between the separate parts of the network and certain administration groups would be enough. You can use automatic assignment of distribution points or assign them manually.
- Building the structure of administration groups, without taking the network topology into account. In this case, you must disable automatic assignment of distribution points and then assign one or several devices to act as distribution points for a root administration group in each of the separate parts of the network, for example, for the **Managed devices** group. All distribution points will be at the same level and will feature the same scope spanning all devices on the organization's network. In this case, each Network Agent will connect to the distribution point that has the shortest route. You can trace the route to a distribution point with the tracert or traceroute utility.

## Standard MSP client configuration: Multiple small remote offices

This standard configuration provides for a number of small remote offices, which may communicate with the head office over the internet. Each remote office is located behind the NAT, that is, connection from one remote office to another is not possible because offices are isolated from one another.

The configuration must be reflected in the structure of administration groups: a separate administration group must be created for each remote office (groups **Office 1** and **Office 2** in the figure below).




Remote offices are included in the administration group structure

One or multiple distribution points must be assigned to each administration group that correspond to an office. Distribution points must be devices at the remote office that have a sufficient amount of free disk space. Devices deployed in the **Office 1** group, for example, will access distribution points assigned to the **Office 1** administration group.

If some users move between offices physically, with their laptops, you must select two or more devices (in addition to the existing distribution points) in each remote office and assign them to act as distribution points for a top-level administration group (**Root group for offices** in the figure above).

Example: A laptop is deployed in the **Office 1** administration group and then is moved physically to the office that corresponds to the **Office 2** administration group. After the laptop is moved, Network Agent attempts to access the distribution points assigned to the **Office 1** group, but those distribution points are unavailable. Then, Network Agent starts attempting to access the distribution points that have been assigned to the **Root group for offices**. Because remote offices are isolated from one another, attempts to access distribution points assigned to the **Root group for offices** administration group will only be successful when Network Agent attempts to access distribution points in the **Office 2** group. That is, the laptop will remain in the administration group that corresponds to the initial office, but the laptop will use the distribution point of the office where it is physically located at the moment.

# Hierarchy of policies, using policy profiles

This section provides information about how to apply policies to devices in administration groups. This section also provides information about policy profiles.

## Hierarchy of policies

In Kaspersky Security Center Linux, you use policies for defining a single collection of settings to multiple devices. For example, the policy scope of application P defined for administration group G includes managed devices with application P installed that have been deployed in group G and all of its subgroups, except for subgroups where the **Inherit from parent group** check box is cleared in the properties.

A policy differs from any local setting by lock icons (🔒) next to its settings. If a setting (or a group of settings) is locked in the policy properties, you must, first, use this setting (or group of settings) when creating effective settings and, second, you must write the settings or group of settings to the downstream policy.

Creation of the effective settings on a device can be described as follows: the values of all settings that have not been locked are taken from the policy, then they are overwritten with the values of local settings, and then the resulting collection is overwritten with the values of locked settings taken from the policy.

Policies of the same application affect each other through the hierarchy of administration groups: Locked settings from the upstream policy overwrite the same settings from the downstream policy.

There is a special policy for out-of-office users. This policy takes effect on a device when the device switches into out-of-office mode. Out-of-office policies do not affect other policies through the hierarchy of administration groups.

## Policy profiles

Applying policies to devices only through the hierarchy of administration groups may be inconvenient in many circumstances. It may be necessary to create several instances of a single policy that differ in one or two settings for different administration groups, and synchronize the contents of those policies in the future.

To help you avoid such problems, Kaspersky Security Center Linux supports *policy profiles*. A policy profile is a named subset of policy settings. This subset is distributed on target devices together with the policy, supplementing it under a specific condition called the *profile activation condition*. Profiles only contain settings that differ from the "basic" policy, which is active on the client device (computer or mobile device). Activation of a profile modifies the policy settings that were active on the device before the profile was activated. The modified settings take values that have been specified in the profile.

The following restrictions are currently imposed on policy profiles:

- A policy can include a maximum 100 profiles.
- A policy profile cannot contain other profiles.
- A policy profile cannot contain notification settings.

Contents of a profile

A policy profile contains the following constituent parts:

- Name Profiles with identical names affect each other through the hierarchy of administration groups with common rules.
- Subset of policy settings. Unlike the policy, which contains all the settings, a profile only contains settings that are actually required (locked settings).
- Activation condition is a logical expression with the device properties. A profile is active (supplements the policy) only when the profile activation condition becomes true. In all other cases, the profile is inactive and ignored. The following device properties can be included in that logical expression:
  - Status of out-of-office mode.
  - Properties of network environment—Name of the active rule for Network Agent connection.
  - Presence or absence of specified tags on the device.
  - Device location in Active Directory unit: explicit (the device is right in the specified OU), or implicit (the device is in an OU, which is within the specified OU at any nesting level).
  - Device's membership in an Active Directory security group (explicit or implicit).
  - Device owner's membership in an Active Directory security group (explicit or implicit).
- Profile disabling check box. Disabled profiles are always ignored and their respective activation conditions are not verified.
- Profile priority. The activation conditions of different profiles are independent, so several profiles can be activated simultaneously. If active profiles contain non-overlapping collections of settings, no problems will arise. However, if two active profiles contain different values of the same setting, an ambiguity will occur. This ambiguity is to be avoided through profile priorities: The value of the ambiguous variable will be taken from the profile that has the higher priority (the one that is rated higher in the list of profiles).

Behavior of profiles when policies affect each other through the hierarchy

Profiles with the same name are merged according to the policy merge rules. Profiles of an upstream policy have a higher priority than profiles of a downstream policy. If editing settings is prohibited in the upstream policy (it is locked), the downstream policy uses the profile activation conditions from the upstream one. If editing settings is allowed in the upstream policy, the profile activation conditions from the downstream policy are used.

Since a policy profile may contain the **Device is offline** property in its activation condition, profiles completely replace the feature of policies for out-of-office users, which will no longer be supported.

A policy for out-of-office users may contain profiles, but its profiles can only be activated after the device switches into out-of-office mode.

## Tasks

Kaspersky Security Center Linux manages Kaspersky security applications installed on devices by creating and running *tasks*. Tasks are required for installing, launching, and stopping applications, scanning files, updating databases and software modules, and performing other actions on applications.

Tasks for a specific application can be created only if the management plug-in for that application is installed.

Tasks can be performed on the Administration Server and on devices.

The following tasks are performed on the Administration Server:

- Automatic distribution of reports
- Downloading of updates to the repository of the Administration Server
- Backup of Administration Server data
- Maintenance of the database

The following types of tasks are performed on devices:

- *Local tasks*—Tasks that are performed on a specific device

  Local tasks can be modified either by the administrator, by using Kaspersky Security Center Web Console, or by the user of a remote device (for example, through the security application interface). If a local task has been modified simultaneously by the administrator and the user of a managed device, the changes made by the administrator will take effect because they have a higher priority.

- *Group tasks*—Tasks that are performed on all devices of a specific group

  Unless otherwise specified in the task properties, a group task also affects all subgroups of the selected group. A group task also affects (optionally) devices that have been connected to secondary and virtual Administration Servers deployed in the group or any of its subgroups.

- *Global tasks*—Tasks that are performed on a set of devices, regardless of whether they are included in any group

For each application, you can create any number of group tasks, global tasks, or local tasks.

You can make changes to the settings of tasks, view the progress of tasks, and copy, export, import, and delete tasks.

A task is started on a device only if the application for which the task was created is running.

Results of tasks are saved in the Syslog event log and the Kaspersky Security Center Linux event log, both centrally on the Administration Server and locally on each device.

Do not include private data in task settings. For example, avoid specifying the domain administrator password.

## Device moving rules

We recommend that you automate the allocation of devices to administration groups through *device moving rules*. A device moving rule consists of three main parts: a name, an execution condition (logical expression with the device attributes), and a target administration group. A rule moves a device to the target administration group if the device attributes meet the rule execution condition.

All device moving rules have priorities. The Administration Server checks the device attributes as to whether they meet the execution condition of each rule, in ascending order of priority. If the device attributes meet the execution condition of a rule, the device is moved to the target group, so the rule processing is complete for this device. If the device attributes meet the conditions of multiple rules, the device is moved to the target group of the rule with the highest priority (that is, has the highest rank in the list of rules).

Device moving rules can be created implicitly. For example, in the properties of an installation package or a remote installation task, you can specify the administration group to which the device must be moved after Network Agent is installed on it. Also, device moving rules can be created explicitly by the administrator of Kaspersky Security Center Linux, in the **Asset management** → **Moving rules** section.

By default, a device moving rule is intended for one-time initial allocation of devices to administration groups. The rule moves devices from the unassigned devices group only once. If a device once was moved by this rule, the rule will never move it again, even if you return the device to the unassigned devices group manually. This is the recommended way of applying moving rules.

You can move devices that have already been allocated to some of the administration groups. To do this, in the properties of a rule, clear the **Move only devices that do not belong to an administration group** check box.

Applying moving rules to devices that have already been allocated to some of the administration groups, significantly increases the load on the Administration Server.

The **Move only devices that do not belong to an administration group** check box is locked in the properties of automatically created moving rules. Such rules are created when you add the *Install application remotely* task or create a stand-alone installation package.

You can create a moving rule that would affect a single device repeatedly.

We strongly recommend that you avoid moving a single device from one group to another repeatedly (for example, in order to apply a special policy to that device, run a special group task, or update the device through a specific distribution point).

Such scenarios are not supported, because they increase the load on Administration Server and network traffic to an extreme degree. These scenarios also conflict with the operating principles of Kaspersky Security Center Linux (particularly in the area of access rights, events, and reports). Another solution must be found, for example, through the use of policy profiles, tasks for device selections, assignment of Network Agents according to the standard scenario.

## Software categorization

The main tool for monitoring the running of applications are *Kaspersky categories* (hereinafter also referred to as *KL categories*). KL categories help Kaspersky Security Center Linux administrators to simplify the support of software categorization and minimize traffic going to managed devices.

User categories must only be created for applications that cannot be classified in any of the existing KL categories (for example, for custom-made software). User categories are created on the basis of an application installation package (MSI) or a folder with installation packages.

If a large collection of software is available, which has not been categorized through KL categories, it may be useful to create an automatically updated category. The checksums of executable files will be automatically added to this category on every modification of the folder containing distribution packages.

# Backup and restoration of Administration Server settings

Backup of the settings of Administration Server and its database is performed through the backup task and klbackup utility. A backup copy includes all the main settings and objects pertaining to the Administration Server, such as certificates, primary keys for encryption of drives on managed devices, keys for various licenses, structure of administration groups with all of its contents, tasks, policies, etc. With a backup copy you can recover the operation of an Administration Server as soon as possible, spending from a dozen minutes to a couple of hours on this.

If no backup copy is available, a failure may lead to an irrevocable loss of certificates and all Administration Server settings. This will necessitate reconfiguring Kaspersky Security Center Linux from scratch, and performing initial deployment of Network Agent on the organization's network again. All primary keys for encryption of drives on managed devices will also be lost, risking irrevocable loss of encrypted data on devices with Kaspersky Endpoint Security. Therefore, do not neglect regular backups of Administration Server using the standard backup task.

The quick start wizard creates a backup task for the Administration Server settings that starts at 4:00 a.m. every day. Backup copies are saved by default in the folder /var/opt/kaspersky/KSC_Backups*.

Because a backup copy contains important data, the backup task and klbackup utility provide for password protection of backup copies. By default, the backup task is created with a blank password. You must set a password in the properties of the backup task. Neglecting this requirement causes a situation where all keys of Administration Server certificates, keys for licenses, and primary keys for encryption of drives on managed devices remain unencrypted.

In addition to the regular backup, you must also create a backup copy prior to every significant change, including installation of Administration Server upgrades and patches.

Restoration from a backup copy is performed with the utility klbackup on an operable instance of Administration Server that has just been installed and has the same version (or later) for which the backup copy was created.

The instance of Administration Server on which the restoration is to be performed, must use a DBMS of the same type and the same or later version. The version of Administration Server can be the same (with an identical or later patch), or later.

This section describes standard scenarios for restoring settings and objects of Administration Server.

## A device with Administration Server is inoperable

If a device with Administration Server is inoperable due to a failure, you are recommended to perform the following actions:

- The new Administration Server must be assigned the same DNS name.

  If a static IP address was set in the Network Agent installation package when Network Agents were deployed, you must also assign the same IP address to the new Administration Server. Alternatively, you can use the connection address that determines the Administration Server to which Network Agent connects (you can obtain this address on managed devices by using the klnagchk utility).

- In the IAM configuration file `var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` , for the `server_iam.ksc_address`, set exactly the same Administration Server address that is specified in the Subject Alternative Name (SAN) of the previously applied Administration Server certificate. Refer to the following article for details: Adding the Administration Server address to the IAM Server configuration.

- Install Administration Server, using a DBMS of the same type, of the same (or later) version. You can install the same version of Server with the same (or later) patch, or a later version. After installation, do not perform the initial setup through the wizard.

- Run the klbackup utility and perform restoration. Reinstall the Web Console after successful restoration.

## The settings of Administration Server or the database are corrupted

If Administration Server is inoperable due to corrupted settings or database (e.g., after a power surge), you are recommended to use the following restoration scenario:

1. Scan the file system on the damaged device.
2. Uninstall the inoperable version of Administration Server.
3. Reinstall Administration Server, using a DBMS of the same type and of the same (or later) version. You can install the same version of Server with the same (or later) patch, or a later version. After installation, do not perform the initial setup through the wizard.
4. Run the klbackup utility and perform restoration.

It is prohibited to restore Administration Server in any way other than through the klbackup utility.

Any attempts to restore Administration Server through third-party software will inevitably lead to desynchronization of data on nodes of the distributed application Kaspersky Security Center Linux and, consequently, to improper functioning of the application.

# About connection profiles for out-of-office users

Out-of-office users of laptops (hereinafter also referred to as "devices") may need to change the method of connecting to an Administration Server or switch between Administration Servers depending on the current location of the device on the enterprise network.

## Using different addresses of a single Administration Server

Devices with Network Agent installed can connect to the Administration Server either from the organization's intranet or from the internet. This situation may require Network Agent to use different addresses for connection to Administration Server: the external Administration Server address for the Internet connection and the internal Administration Server address for the internal network connection.

To do this, you must add a profile (for connection to Administration Server from the Internet) to the Network Agent policy. Add the profile in the policy properties (**Connectivity** section, **Connection profiles** subsection). In the profile creation window, you must disable the **Use to receive updates only** option and select the **Synchronize connection settings with the Administration Server settings specified in this profile** option. If you use a connection gateway to access Administration Server (for example, in a Kaspersky Security Center Linux configuration as that described in Internet access: Network Agent as connection gateway in DMZ), you must specify the address of the connection gateway in the corresponding field of the connection profile.

## Switching between Administration Servers depending on the current network

If the organization has multiple offices with different Administration Servers and some of the devices with Network Agent installed move between them, you need Network Agent to connect to the Administration Server of the local network in the office where the device is currently located.

In this case, you must create a profile for connection to Administration Server in the properties of the policy of Network Agent for each of the offices, except for the home office where the original home Administration Server is located. You must specify the addresses of Administration Servers in connection profiles and enable or disable the **Use to receive updates only** option:

- Select the option if you need Network Agent to be synchronized with the home Administration Server, while using the local Server for downloading updates only.
- Disable this option if it is necessary for Network Agent to be managed completely by the local Administration Server.

After that, you must set up the conditions of switching to the newly created profiles: at least one condition for each of the offices, except for the home office. Every condition's purpose consists in detection of items that are specific for an office's network environment. If a condition is true, the corresponding profile gets activated. If none of the conditions is true, Network Agent switches to the home Administration Server.

# About switching Network Agent to other Administration Servers

Kaspersky Security Center Linux provides the option of switching Network Agent on a client device to other Administration Servers if the following settings of the network have been changed:

- **Condition for DHCP server address**—The IP address of the network Dynamic Host Configuration Protocol (DHCP) server has changed.

  The **Condition for DHCP server address** setting is currently not available.

- **Condition for default connection gateway address**—The address of the main network gateway has changed.
- **Condition for DNS domain**—The DNS suffix of the subnet has changed.
- **Condition for DNS server address**—The IP address of the network DNS server has changed.
- **Condition for WINS server address**—The IP address of the network WINS server has changed. This setting is available only for devices running Windows.
- **Condition for name resolvability**—The DNS or NetBIOS name of the client device has changed.
- **Condition for subnet**—Changes the subnet address and mask.
- **Condition for Windows domain accessibility**—Changes the status of the Windows domain to which the client device is connected. This setting is available only for devices running Windows.
- **Condition for SSL connection address accessibility**—The client device can or cannot (depending on the option that you select) establish an SSL connection with a specified server (name:port). You must use a dedicated server with software capable of handling high load and frequent Network Agent requests for the connection. Do not specify the Administration Server's port. For each server, you can additionally specify an SSL certificate. In this case, the Network Agent verifies the server certificate in addition to checking the capability of an SSL connection. If the certificate does not match, the connection fails.

The initial settings of the Network Agent connection to Administration Server are defined when installing the Network Agent. Afterwards, if rules for switching the Network Agent to other Administration Servers have been created, the Network Agent responds to changes in the network settings as follows:

- If the network settings comply with one of the rules created, Network Agent connects to the Administration Server specified in this rule. Applications installed on client devices switch to out-of-office policies, provided such behavior is enabled by a rule.
- If none of the rules apply, Network Agent reverts to the default settings of connection to the Administration Server specified during the installation. Applications installed on client devices switch back to active policies.
- If the Administration Server is not accessible, Network Agent uses out-of-office policies.

Network Agent switches to the out-of-office policy only if the **Enable out-of-office mode when Administration Server is not available** option is enabled in the Network Agent policy settings.

The settings of Network Agent connection to Administration Server are saved in a connection profile. In the connection profile, you can create rules for switching client devices to out-of-office policies, and you can configure the profile so that it could only be used for downloading updates.

# Creating a connection profile for out-of-office users

*To create a profile for connecting Network Agent to Administration Server for out-of-office users:*

1. If you want to create a connection profile for a group of managed devices, open the Network Agent policy of this group. To do this, do the following:

   a. In the main menu, go to **Asset management** → **Policies**.

   b. Select the administration group for which the connection profile is to be created:

   - For the root group, you can proceed to the next step.
   - For a subgroup, click the **Show hierarchy** button at the top of the page, and then in the window that opens, click the name of the required subgroup.

   The path to the selected group is displayed at the top of the page. If necessary, you can click a link with the administration group name to go to the group. By default, the last link in the path is inactive. Also, you can close the hierarchy window by clicking the **Hide hierarchy** button.

   c. Add the Network Agent policy for the group of managed devices. If you have already created it, click the Network Agent policy name to open the policy properties.

2. If you want to create a connection profile for a specific managed device, do the following:

   a. In the main menu, go to **Asset management** → **Managed devices**.

   b. Click the name of the managed device.

   c. In the managed device properties window that opens, go to the **Applications** tab.

   d. Click the name of the Network Agent policy to which only the selected managed device applies.

3. In the properties window that opens, go to **Application settings** → **Connectivity** → **Connection profiles.**

4. In the **Administration Server connection profiles** section, click the **Add** button.

   By default, the list of connection profiles contains the <Offline mode> and <Home Administration Server> profiles. Profiles cannot be edited or removed.

   The <Offline mode> profile does not specify any Server for connection. Therefore, Network Agent, when switched to that profile, does not attempt to connect to any Administration Server while applications installed on client devices run under out-of-office policies. The <Offline mode> profile can be used if devices are disconnected from the network.

   The <Home Administration Server> profile specifies the connection for the Administration Server that was selected during Network Agent installation. The <Home Administration Server> profile is applied when a device is reconnected to the home Administration Server after it was running on an external network for some time.

5. In the **Configure profile** window that opens, configure the connection profile:

- **Profile name**

  In the entry field you can view or change the connection profile name.

- **Administration Server address**

  Address of the Administration Server to which the client device must connect during profile activation.

- **Port number**

  Port number that is used for connection.

- **SSL port**

  Port number for connection if using the SSL protocol.

- **Use SSL connection**

  If this option is enabled, the connection is established through a secure port, by using SSL protocol.

  By default, this option is enabled. We recommend that you do not disable this option so your connection remains secured.

- Select the **Use proxy server** option if you want to use a proxy server when connecting to the internet. If this option is selected, fields are available for entering settings. Specify the following settings for a proxy server connection:

  - **Address**

    Address of the proxy server used for Kaspersky Security Center Linux connection to the internet.

  - **Port number**

    Number of the port through which Kaspersky Security Center Linux proxy connection will be established.

  - **Proxy server authentication**

    If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

  - **User name**

    User account under which connection to the proxy server is established (this field is available if the **Proxy server authentication** check box is selected).

  - **Password**

    Password set by the user under whose account the proxy server connection is established (this field is available if the **Proxy server authentication** check box is selected).

    To see the entered password, click and hold the **Show** button for as long as you require.

- **Connection gateway address**

  Address of the gateway through which client devices connect to the Administration Server.

- **Enable out-of-office mode when Administration Server is not available**

  Select this check box to allow the applications installed on a client device to use policy profiles for devices in out-of-office mode, as well as out-of-office policies, at any connection attempt if the Administration Server is not available. If no out-of-office policy has been defined for the application, the active policy will be used.

  If this option is disabled, applications will use active policies.

  This check box is cleared by default.

- **Use to receive updates only**

  If this option is enabled, the profile will only be used for downloading updates by applications installed on the client device. For other operations, connection to the Administration Server will be established with the initial connection settings defined during Network Agent installation.

  By default, the option is enabled.

- **Synchronize connection settings with the Administration Server settings specified in this profile**

  If this option is enabled, Network Agent connects to Administration Server using the settings specified in the profile properties.

  If this option is disabled, Network Agent connects to Administration Server using the original settings that have been specified during installation.

  This option is available if the **Use to receive updates only** option is disabled.

  By default, this option is disabled.

A profile for connecting Network Agent to Administration Server is created for out-of-office users. When Network Agent connects to Administration Server by using this profile, applications installed on the client device will use policies for devices in out-of-office mode or out-of-office policies.

# Remote access to managed devices

This section provides information about remote access to managed devices.

## Using the "Do not disconnect from the Administration Server" option to provide continuous connectivity between a managed device and the Administration Server

If you do not use push servers, Kaspersky Security Center Linux does not provide continuous connectivity between managed devices and the Administration Server. Network Agents on managed devices periodically establish connections and synchronize with the Administration Server. The interval between those synchronization sessions is defined in a Network Agent policy. If an early synchronization is required, the Administration Server (or a distribution point, if it is in use) sends a signed network packet over an IPv4 or IPv6 network to the UDP port of the Network Agent. By default, the port number is 15000. If no connection through UDP is possible between the Administration Server and a managed device, synchronization will run at the next regular connection of Network Agent to the Administration Server within the synchronization interval.

Some operations cannot be performed without an early connection between Network Agent and the Administration Server, such as running and stopping local tasks or receiving statistics for a managed application. To resolve this issue, if you are not using push servers, you can use the **Do not disconnect from the Administration Server** option to make sure that there is continuous connectivity between a managed device and the Administration Server.

*To provide continuous connectivity between a managed device and the Administration Server:*

1. In the main menu, go to **Asset management** → **Managed devices**.

   The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the required device.

3. In the device properties window, in the **General** section, enable the **Do not disconnect from the Administration Server** option.

Continuous connectivity is established between the managed device and the Administration Server.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

# About checking the time of connection between a device and the Administration Server

Upon shutting down a device, Network Agent notifies the Administration Server of this event. In Kaspersky Security Center Web Console that device is displayed as shut down. However, Network Agent cannot notify Administration Server of all such events. The Administration Server, therefore, periodically analyzes the **Connected to Administration Server** attribute (the value of this attribute is displayed in Kaspersky Security Center Web Console, in the device properties, in the **General** section) for each device and compares it against the synchronization interval from the current settings of Network Agent. If a device has not responded over more than three successive synchronization intervals, that device is marked as shut down.

# About forced synchronization

Although Kaspersky Security Center Linux automatically synchronizes the status, settings, tasks, and policies for managed devices, in some cases the administrator needs to know exactly whether synchronization has already been performed for a specified device at the present moment.

The properties window of a managed device contains the **Force synchronization** button. When Kaspersky Security Center Linux executes the synchronization command, the Administration Server attempts to connect to the device. If this attempt is successful, forced synchronization will be performed. Otherwise, synchronization will be forced only after the next scheduled connection between Network Agent and the Administration Server.

# Sizing Guide

This section provides information about Kaspersky Security Center Linux sizing.

# About this Guide

Kaspersky Security Center Linux (also referred to as Kaspersky Security Center) Sizing Guide is intended for professionals who install and administer Kaspersky Security Center, as well as for those who provide technical support to organizations that use Kaspersky Security Center.

All recommendations and calculations are given for networks on which Kaspersky Security Center manages the protection of devices with Kaspersky software installed.

To obtain and maintain optimum performance under varying operational conditions, you must take into account the number of networked devices, network topology, and set of Kaspersky Security Center features that you require.

This Guide provides the following information:

- Limitations of Kaspersky Security Center
- Calculations for the key nodes of Kaspersky Security Center (Administration Servers and distribution points):
  - Hardware requirements for Administration Servers and distribution points
  - Calculation of the number and configuration of Administration Servers
  - Calculating the number and configuration of distribution points
- Configuration of event logging in the database depending on the number of networked devices
- Common best practices for performance optimization
- Configuration of specific tasks aimed at optimal performance of Kaspersky Security Center
- Traffic rate (network load) between Kaspersky Security Center Administration Server and every protected device

Consulting this guide is recommended in the following cases:

- When planning resources prior to Kaspersky Security Center installation
- When planning significant changes to the scale of the network on which Kaspersky Security Center is deployed
- When switching from using Kaspersky Security Center within a limited network segment (a test environment) to full-scale deployment of Kaspersky Security Center on the corporate network
- When making changes to the set of Kaspersky Security Center features used

# Limitations of Kaspersky Security Center Linux

The following table displays the limitations of the current version of Kaspersky Security Center Linux.

Limitations of Kaspersky Security Center Linux

| Type of limitation | Value |
|---|---|
| Maximum number of managed devices per Administration Server | 50,000 |
| Maximum number of devices with the **Do not disconnect from the Administration Server** option selected | 300 |
| Maximum number of administration groups | 10,000 |
| Maximum number of events to store | 45,000,000 |
| Maximum number of policies | 2000 |
| Maximum number of tasks | 2000 |
| Maximum number of profiles in a policy | 100 |
| Maximum number of secondary Administration Servers on a single primary Administration Server | 500 |
| Maximum number of virtual Administration Servers | 500 |
| Maximum number of devices that one distribution point can serve | 10,000 |
| Maximum number of devices that may use a single connection gateway | 10,000, including mobile devices |
| Maximum number of mobile devices per Administration Server | 100,000 minus the number of stationary managed devices |

# Calculations for Administration Servers

This section provides the software and hardware requirements for devices used as Administration Servers. Also provided are recommendations for calculating the number and hierarchy of Administration Servers depending on the configuration of the organization's network.

We recommend that after installing Administration Server and DBMS on the devices, you install Kaspersky Endpoint Security for Linux on these devices. For Kaspersky Endpoint Security hardware requirements, refer to Kaspersky Endpoint Security for Linux Help.

The load created by Kaspersky Endpoint Security for Linux when integrated with Managed Detection and Response and Kaspersky Endpoint Detection and Response Expert (on-premise) is not taken into account in the calculations for concurrent installation of Kaspersky Security Center Linux and KES_LIN>.

## Calculation of hardware resources for the Administration Server

This section contains calculations that provide guidance for planning hardware resources for the Administration Server.

# Hardware requirements for the DBMS and the Administration Server

The following tables give the recommended minimum hardware requirements to a DBMS and Administration Server obtained during tests. For a complete list of operating systems and DBMSs supported, please refer to the list of hardware and software requirements.

You have to turn on the swap file on the device with Administration Server installed. The swap file minimum size must be 1.5 times greater than the RAM volume.

After installing Administration Server an the DBMS on a device, we recommend installing Kaspersky Endpoint Security for Linux.
For the concurrent installation, you must have minimum 300 IOPS as well as add to the Administration Server requirements 1,5 GB of RAM, and 15% to the CPU.
For hardware requirements of Kaspersky Endpoint Security, refer to the Kaspersky Endpoint Security for Linux Help.

For information about the security settings required to work with Kaspersky Security Center Linux, refer to the Kaspersky Endpoint Security for Linux Help.

## The network includes 50,000 devices

Configuration of the device that has Administration Server installed

| Hardware | Value |
|---|---|
| CPU | 8 cores (12 cores recommended), 2500 MHz |
| RAM | 16 GB |
| Disk space | 300 GB, 150 IOPS or higher |

Configuration of the device that has PostgreSQL DBMS installed

| Hardware | Value |
|---|---|
| CPU | 16 cores, 2500 MHz |
| RAM | 32 GB |
| Disk space | 300 GB, 150 IOPS or higher |

Configuration of nodes for a failover cluster

| Hardware | Value |
|---|---|
| CPU | 8 cores (12 cores recommended), 2500 MHz |
| RAM | 16 GB |
| Disk space | 300 GB, 150 IOPS or higher |
| Network interface controller | 1 Gbps |

Configuration of the device that has both Administration Server and PostgreSQL DBMS installed

| Hardware | Value |
|---|---|
| CPU | 24 cores (28 cores recommended), 2500 MHz |
| RAM | 48 GB |
| Disk space | 600 GB, 300 IOPS or higher |

## The network includes 30,000 devices

Configuration of the device that has Administration Server installed

| Hardware | Value |
|---|---|
| CPU | 6 cores (8 cores recommended), 2500 MHz |
| RAM | 12 GB |
| Disk space | 200 GB, 150 IOPS or higher |

Configuration of the device that has PostgreSQL DBMS installed

| Hardware | Value |
|---|---|
| CPU | 12 cores, 2500 MHz |
| RAM | 22 GB |
| Disk space | 250 GB, 150 IOPS or higher |

Configuration of nodes for a failover cluster

| Hardware | Value |
|---|---|
| CPU | 6 cores (8 cores recommended), 2500 MHz |
| RAM | 12 GB |
| Disk space | 200 GB, 150 IOPS or higher |
| Network interface controller | 1 Gbps |

Configuration of the device that has both Administration Server and PostgreSQL DBMS installed

| Hardware | Value |
|---|---|
| CPU | 16 cores (20 cores recommended), 2500 MHz |
| RAM | 34 GB |
| Disk space | 450 GB, 300 IOPS or higher |

## The network includes 10,000 devices

Configuration of the device that has Administration Server installed

| Hardware | Value |
|---|---|
| CPU | 4 cores (6 cores recommended), 2500 MHz |
| RAM | 8 GB |
| Disk space | 100 GB, 150 IOPS or higher |

Configuration of the device that has PostgreSQL DBMS installed

| Hardware | Value |
|---|---|
| CPU | 6 cores, 2500 MHz |
| RAM | 10 GB |
| Disk space | 200 GB, 150 IOPS or higher |

Configuration of nodes for a failover cluster

| Hardware | Value |
|---|---|
| CPU | 4 cores (6 cores recommended), 2500 MHz |
| RAM | 8 GB |
| Disk space | 100 GB, 150 IOPS or higher |
| Network interface controller | 1 Gbps |

Configuration of the device that has both Administration Server and PostgreSQL DBMS installed

| Hardware | Value |
|---|---|
| CPU | 8 cores (14 cores recommended), 2500 MHz |
| RAM | 18 GB |
| Disk space | 300 GB, 300 IOPS or higher |

## The network includes 1000 devices

Configuration of the device that has Administration Server installed

| Hardware | Value |
|---|---|
| CPU | 2 cores, 2500 MHz |
| RAM | 6 GB |
| Disk space | 10 GB, 150 IOPS or higher |

Configuration of the device that has PostgreSQL DBMS installed

| Hardware | Value |
|---|---|
| CPU | 2 cores, 2500 MHz |
| RAM | 4 GB |
| Disk space | 20 GB, 150 IOPS or higher |

Configuration of nodes for a failover cluster

| Hardware | Value |
|---|---|
| CPU | 2 cores, 2500 MHz |
| RAM | 6 GB |
| Disk space | 10 GB, 150 IOPS or higher |
| Network interface controller | 1 Gbps |

Configuration of the device that has both Administration Server and PostgreSQL DBMS installed

| Hardware | Value |
|---|---|
| CPU | 4 cores, 2500 MHz |
| RAM | 10 GB |
| Disk space | 30 GB, 300 IOPS or higher |

The tests were run under the following settings:

- Automatic assignment of distribution points is enabled on the Administration Server, or distribution points are assigned manually in accordance with the recommended table.
- The PostgreSQL DBMS does not include any extensions other than plpgsql.

On the device that has DBMS installed, the database consumes approximately 100 GB of disk space, and the transaction log consumes approximately 200 GB of disk space.

## Calculation of database space

The approximate amount of space that must be reserved in the database can be calculated using the following formula:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

where:

- C is the number of devices.

  If the managed devices include dynamic virtual machines, C is the sum of the number of non-dynamic managed devices and the number of dynamic virtual machines with Network Agent created between two consecutive runs of the **Administration Server maintenance** task.

- E is the number of events to store.
- A is the total number of Active Directory objects:
  - Device accounts
  - User accounts
  - Accounts of security groups
  - Active Directory organizational units

  If scanning of Active Directory is disabled, A is considered to equal zero.
- N is the average number of inventoried executable files on an endpoint device.
- F is the number of endpoint devices, where executable files were inventoried.

If you plan to enable (in the Kaspersky Endpoint Security policy settings) notification of Administration Server on applications that you run, you will need additional (0.03 * C) gigabytes to store in the database the information about applications that you run.

During operation, a certain *unallocated space* is always present in the database. Therefore, the actual size of the database file often turns out to be approximately twice as large as the amount of space occupied in the database.

It is not recommended to limit explicitly the size of the transaction log. It is recommended to leave the default value of the MAXSIZE parameter.

## Calculation of disk space

The Administration Server disk space required for the /var/opt/kaspersky/klnagent_srv/ folder can be estimated approximately using the formula:

(724 * C + 0.15 * E + 0.17 * A), KB

where:

- C is the number of devices.

  If the managed devices include dynamic virtual machines, C is the sum of the number of non-dynamic managed devices and the number of dynamic virtual machines with Network Agent created between two consecutive runs of the **Administration Server maintenance** task.

- E is the number of events to store.
- A is the total number of Active Directory objects:
  - Device accounts
  - User accounts
  - Accounts of security groups
  - Active Directory organizational units

If scanning of Active Directory is disabled, A is considered to equal zero.

# Calculation of the number and configuration of Administration Servers

To reduce the load on the primary Administration Server, you can assign a separate Administration Server to each administration group. The number of secondary Administration Servers cannot exceed 500 for a single primary Administration Server.

We recommend that you create the configuration of Administration Servers in correspondence to the configuration of your organization's network.

# Recommendations for connecting dynamic virtual machines to Kaspersky Security Center

Dynamic virtual machines (also referred to as dynamic VMs) consume more resources than static virtual machines.

For more information on dynamic virtual machines, see Support of dynamic virtual machines.

When a new dynamic VM is connected, Kaspersky Security Center Linux creates a record for this dynamic VM in Kaspersky Security Center Web Console and moves the dynamic VM to the administration group. After that, the dynamic VM is added to the Administration Server database. The Administration Server is fully synchronized with Network Agent installed on this dynamic VM.

In an organization's network, Network Agent creates the following network lists for each dynamic VM:

- Hardware
- Installed software
- Detected vulnerabilities
- Events and lists of executable files of the Application control component

The Network Agent transfers these network lists to the Administration Server. The size of the network lists depends on components installed on the dynamic VM, and may affect the performance of Kaspersky Security Center Linux and database management system (DBMS). Note that the load can grow non-linearly.

After the user finishes working with the dynamic VM and turns it off, this machine is then removed from the virtual infrastructure and entries about this machine are removed from the Administration Server database.

All these actions consume a lot of Kaspersky Security Center Linux and Administration Server database resources, and can reduce the performance of Kaspersky Security Center Linux and DBMS. We recommend that you connect up to 20,000 dynamic VMs to Kaspersky Security Center Linux.

You can connect more than 20,000 dynamic VMs to Kaspersky Security Center Linux if the connected dynamic VMs perform standard operations (for example, database updates) and consume no more than 80 percent of memory and 75–80 percent of available cores.

Changing policy settings, software or operating system on the dynamic VM can reduce or increase resource consumption. The consumption of 80–95 percent of resources is considered optimal.

# Calculations for distribution points and connection gateways

This section provides the hardware requirements for devices used as distribution points together with recommendations for calculating the number of distribution points and connection gateways depending on the configuration of the corporate network.

## Requirements for a distribution point

Hardware and software requirements for Windows and Linux-based distribution points are described in this article.

If any remote installation tasks are pending on the Administration Server, the device with the distribution point will also require an amount of free disk space that is equal to the total size of the installation packages to be installed.

If one or multiple instances of the task for update (patch) installation and vulnerability fix are pending on the Administration Server, the device with the distribution point will also require additional free disk space, equal to twice the total size of all patches to be installed.

If you use the scheme where distribution points receive database updates and application software modules directly from Kaspersky update servers, the distribution points must be connected to the internet.

It is not recommended to assign the Administration Server as a distribution point, as this will increase the load on the Administration Server.

### Hardware requirements for Windows-based distribution points

**Minimum hardware requirements for Windows-based distribution points**

| Number of client devices | CPU | RAM | RAM, with patch management enabled | Disk space |
|---|---|---|---|---|
| 10,000 | 4 cores, 2500 MHz | 8 GB | 8 GB | 120 GB |
| 5000 | 4 cores, 2500 MHz | 6 GB | 8 GB | 120 GB |
| 1000 | 2 cores, 2500 MHz | 4 GB | 8 GB | 120 GB |

### Hardware requirements for Linux-based distribution points

**Minimum hardware requirements for Linux-based distribution points**

| Number of client devices | CPU | RAM | Disk space |
|---|---|---|---|
| 10,000 | 4 cores, 2500 MHz | 10 GB | 120 GB |
| 5000 | 4 cores, 2500 MHz | 8 GB | 120 GB |
| 1000 | 2 cores, 2500 MHz | 6 GB | 120 GB |

## Calculating the number and configuration of distribution points

The more client devices a network contains, the more distribution points it requires. We recommend that you not disable automatic assignment of distribution points. When automatic assignment of distribution points is enabled, Administration Server assigns distribution points if the number of client devices is quite large and defines their configuration.

### Using exclusively assigned distribution points

If you plan to use certain specific devices as distribution points (that is, exclusively assigned servers), you can opt out of using automatic assignment of distribution points. In this case, make sure that the devices that you intend to make distribution points have sufficient volume of free disk space, are not shut down regularly, and have Sleep mode disabled.

Number of dedicated distribution points in a network containing one network segment, depending on the number of devices in the network

| Number of client devices per network segment | Number of distribution points |
|---|---|
| Less than 300 | 0 (Do not assign distribution points) |
| More than 300 | Acceptable: (N/10,000 + 1), recommended: (N/5000 + 2), where N is the number of networked devices |

Number of dedicated distribution points in a network containing multiple network segments, depending on the number of devices in the network

| Number of client devices in each network segment | Number of distribution points |
|---|---|
| Less than 10 | 0 (Do not assign distribution points) |
| 10–100 | 1 |
| More than 100 | Acceptable: (N/10,000 + 1), recommended: (N/5000 + 2), where N is the number of networked devices |

### Using standard client devices (workstations) as distribution points

If you plan to use standard client devices (that is, workstations) as distribution points, we recommend that you assign distribution points as shown in the tables below in order to avoid excessive load on the communication channels and on Administration Server:

Number of workstations functioning as distribution points on a network that contains a single network segment, based on the number of networked devices

| Number of client devices per network segment | Number of distribution points |
|---|---|
| Less than 300 | 0 (Do not assign distribution points) |
| More than 300 | (N/300 + 1), where N is the number of networked devices; there must be at least 3 distribution points |

Number of workstations functioning as distribution points on a network that contains multiple network segments, based on the number of networked devices

| Number of client devices per network segment | Number of distribution points |
|---|---|
| Less than 10 | 0 (Do not assign distribution points) |
| 10–30 | 1 |
| 31–300 | 2 |
| More than 300 | (N/300 + 1), where N is the number of networked devices; there must be at least 3 distribution points |

If a distribution point is shut down (or not available for some other reason), the managed devices in its scope can access the Administration Server for updates.

## Calculation of the number of connection gateways

If you plan to use a connection gateway, we recommend that you designate a special device for this function.

A connection gateway can cover a maximum 10,000 managed devices.

# Logging information about events for tasks and policies

This section provides calculations associated with event storage in the database of the Administration Server and offers recommendations on how to minimize the number of events, thereby reducing the load on the Administration Server.

By default, the properties of each task and policy provide for storing all events related to task execution and policy enforcement.

However, if a task is run quite frequently (for example, more than once per week) and on a fairly large number of devices (for example, more than 10,000), the number of events may turn out to be too large and the events may flood the database. In this case, we recommend selecting one of two options in the task settings:

- **Save events related to task progress**. In this case, the database receives only information about task launch, progress, and completion (successful, with a warning or error) from each device on which the task is run.

- **Save only task execution results**. In this case, the database receives only information about task completion (successful, with a warning or error) from each device on which the task is run.

If a policy has been defined for a fairly large number of devices (for example, more than 10,000), the number of events may also turn out to be large, and the events may flood the database. In this case, it is recommended to choose only the most critical events in the policy settings and enable their logging. You are advised to disable the logging of all other events.

In doing so, you will reduce the number of events in the database, increase the speed of execution of scenarios associated with analysis of the event table in the database, and lower the risk that critical events will be overwritten by a large number of events.

You can also reduce the storage term for events associated with a task or a policy. The default period is 7 days for task-related events and 30 days for policy-related events. When changing the event storage term, consider the work procedures in place at your organization and the amount of time that the system administrator can devote to analyzing each event.

It is advisable to modify the event storage settings in any of the following cases:

- Events about changes in the intermediate states of group tasks and events about applying policies occupy a large share of all events in the Kaspersky Security Center Linux database.

- The operating system log begins showing entries about automatic removal of events when the established limit on the total number of events stored in the database is exceeded.

Choose event logging options based on the assumption that the optimal number of events coming from a single device per day must not exceed 20. You can increase this limit slightly, if necessary, but only if the number of devices on your network is relatively small (fewer than 10,000).

# Best practices for an Administration Server that manages a large number of devices

## Best practices for using DBMS

Configure the **Administration Server maintenance** task to be run on a regular basis, especially if you use a PostgreSQL DBMS.

Exclude the DBMS folder from IOC scanning.

## Best practices for policies and profiles

Reduce the number of active policies for a component (such as Kaspersky Endpoint Security for Windows). You can replace policies with policy profiles.

## Best practices for an Administration Server that manages a large number of devices

Reduce the number of simultaneously run tasks, especially remote installation and patch management.

Reduce the number and optimize the schedule for tasks that operate on device selections.

In the **Event configuration** section of policy settings, minimize the number of event types being saved.

## Best practices for storing events

Reduce the frequency of single-type events from the Application Control component. Refer to the following article for details: About blocking frequent events.

Reduce the storage term for events from components (such as Kaspersky Endpoint Security for Windows) and informational events about fixed vulnerabilities.

Enable the **Save events related to task progress** setting in the task properties for general tasks such as update tasks. Refer to the following article for details: Logging of information about events for tasks and policies.

Optimize the inventory task settings. Refer to the following article for details: Inventory task.

# Specific considerations and optimal settings of certain tasks

Certain tasks are subject to specific considerations related to the number of networked devices. This section offers recommendations on the optimal configuration of settings for such tasks.

Device discovery, the data backup task, database maintenance task, and group tasks for updating Kaspersky Endpoint Security are part of the basic functionality of Kaspersky Security Center Linux.

The inventory task is part of the Vulnerability and patch management feature and is unavailable if this feature is not activated.

## Device discovery frequency

It is not advisable to increase the default frequency of device discovery because this can create an excessive load on domain controllers. Instead, it is recommended to schedule polling at the minimum possible frequency permitted by the needs of your organization. Recommendations for calculating the optimal schedule are provided in the table below.

Device discovery schedule

| Number of networked devices | Recommended device discovery frequency |
|---|---|
| Less than 10,000 | Default frequency or less |
| 10,000 or greater | Once per day or less |

## Administration Server data backup task and database maintenance task

The Administration Server stops working when the following tasks are running:

- Backup copying of Administration Server data
- Administration Server maintenance

When these tasks are running, the database cannot receive any data.

You may have to reschedule these tasks so that they are not executed at the same time as other Administration Server tasks.

## Group tasks for updating Kaspersky Endpoint Security

If the Administration Server acts as the update source, the recommended schedule option for group update tasks of Kaspersky Endpoint Security 10 and later versions is **When new updates are downloaded to the repository** with the **Use automatically randomized delay for task starts** check box selected.

If a local task for downloading updates from Kaspersky servers to the repository is created on each distribution point, periodic scheduling is recommended for the Kaspersky Endpoint Security group update task. The value of the randomization period must be one hour in this case.

## Inventory task

You can reduce load on the database while obtaining information about the executable files. To do this, we recommend that you run an inventory task for Kaspersky Endpoint Security on reference devices on which a standard set of software is installed.

The number of executable files received by the Administration Server from a single device cannot exceed 150,000. When Kaspersky Security Center Linux reaches this limit, it cannot receive any new files.

Typically, the number of files on a common client device does not exceed 60,000. The number of executable files on a file server can be greater than and even exceed the 150,000 threshold.

# Details of network load spread among Administration Server and protected devices

This section provides the results of test measurements of network traffic with a description of the conditions under which the measurements were performed. You can refer to this information when planning the network infrastructure and the throughput capacity of network channels within your organization (or between the Administration Server and another organization with devices to protect). Knowing the throughput capacity of the network, you can also estimate approximately how much time different data transmission operations will take.

## Traffic rate under various scenarios

The table below shows the results of measuring tests conducted on traffic between the Administration Server and a managed device in different scenarios.

By default, devices are synchronized with the Administration Server every 15 minutes or at a longer interval. However, if you modify the settings of a policy or a task on the Administration Server, early synchronization occurs on devices to which the policy (or task) is applicable so the new settings are transmitted to the devices.

Traffic rate between the Administration Server and managed device

| Scenario | Traffic from the Administration Server to each managed device | Traffic from each managed device to the Administration Server |
|---|---|---|
| Installing Kaspersky Endpoint Security for Linux with updated databases | 390 MB | 3.3 MB |
| Network Agent installation | 75 MB | 397 KB |
| Concurrent installation of Network Agent and Kaspersky Endpoint Security for Linux | 459 MB | 3.6 MB |
| Initial update of anti-virus databases without updating the databases in the package (if participation in Kaspersky Security Network is disabled) | 113 MB | 1,8 MB |

| Scenario | Traffic from the Administration Server to each managed device | Traffic from each managed device to the Administration Server |
|---|---|---|
| Daily update of anti-virus databases (if participation in Kaspersky Security Network is enabled) | 22 MB | 373 MB |
| Initial synchronization before update of databases on a device (transfer of policies and tasks) | 382 KB | 446 KB |
| Initial synchronization after updating databases on a device | 20 KB | 157 KB |
| Synchronization with no changes on the Administration Server (according to schedule) | 18 KB | 23 KB |
| Synchronization when a single setting in a group policy is changed (as soon as the setting is altered) | 19 KB | 20 KB |
| Synchronization when a single setting in a group task is changed (as soon as the setting is altered) | 14 KB | 11 KB |
| Forced synchronization | 110 KB | 109 KB |
| **Virus detected** event (1 virus) | 44 KB | 50 KB |
| **Virus detected** event (10 viruses) | 58 KB | 77 KB |
| One-time traffic after enabling the Application Registry list | up to 10 KB | up to 12 KB |
| Everyday traffic when the Application Registry list is enabled | up to 840 KB | up to 1 MB |

# Average traffic usage per 24 hours

The average 24-hour traffic usage between the Administration Server and a managed device is as follows:

- Traffic from the Administration Server to the managed device is 840 KB.
- Traffic from the managed device to the Administration Server is 1 MB.

The traffic was measured under the following conditions:

- The managed device had Network Agent and Kaspersky Endpoint Security for Linux installed.
- The device was not assigned a distribution point.
- Vulnerability and patch management was not enabled.
- The frequency of synchronization with the Administration Server was 15 minutes.

# Known issues and limitations

Kaspersky Security Center Linux has the following limitations, which are not critical to operation of the application:

- 8698100: the **Backup of Administration Server data** task ends with the error "Check if SQL Server has access to the destination folder" when using two-way authentication between the klpg_dump utility and PostgreSQL.
- 10253149: In the properties of the Kaspersky Endpoint Security for Windows policy (**Event configuration** → **Warnings**), when transitioning to the properties of the **Task interrupted** event type, the text in the expandable text about the mass event attribute is not displayed.
- 10723777: When updating databases using the **Download updates to the Administration Server repository**, Kaspersky Security Center Linux attempts to use databases with a localization different from that of Kaspersky Security Center Linux, if the localization is not English (en).
- 10427694: On Ubuntu 24.04, due to issues with the processing of asynchronous system calls, the Administration Server mistakenly generates dumps.
- 10007954: After creating and starting the **Find vulnerabilities and required updates** task, when navigating to the task results on the secondary Server, the "Connection to the Administration Server has been interrupted" error occurs.
- 10671377: When using PostgreSQL or Postgres Pro 18.1–18.5, running tasks may terminate with the error "'[53000]' ERROR: no empty local buffer available". We recommend upgrading PostgreSQL to version 18.6 or following these steps:

  1. Stop the Administration Server service.
  2. Stop the DBMS service.
  3. Add add the following line to the end of the postgresql.conf file : `[[effective_io_concurrency=0]]`.
  4. Start the DBMS service.
  5. Verify that the value of the `effective_io_concurrency` setting is `0` by running the following query:
     `SELECT setting FROM pg_settings WHERE name = 'effective_io_concurrency';`
  6. Start the Administration Server service.

- 10564198: When upgrading Kaspersky Security Center Linux to version 16.3 on nodes of a Kaspersky Security Center Linux failover cluster, running the postinstall.pl script to configure the Administration Server may lead to installation errors.
- 8994760: If you have access rights on virtual Administration Servers but you do not have access rights on the primary Administration Server and you try to log in to Kaspersky Security Center Linux, an error occurs and the error message **Your request cannot be processed right now. Please wait and then try again** is incorrectly displayed. The error text must be the following: **Check your access rights. You must have access rights on the primary server or on one of the virtual servers only. Contact the main administrator, and then try again**
- 10302954: When specifying the conditions for a device moving rule, if on the **Network** tab, you enable the **Device is located in a subgroup of the Domains group** setting, the drop-down list of subgroups is displayed empty.

- 10253149: For application policies, if on the **Event configuration** tab you select a mass event, the **Show more** expanding block with a warning about the effect of such events on Administration Server or the DBMS performance is not displayed.

- 9302142: The **Use Network Agent as a connection gateway in DMZ** option is not supported on Microsoft Windows on Arm.

- 9065814: An error may occur when attempting domain authentication from a Windows-based device in a Samba 4 domain.

- 9335676: After switching the primary node in a high-availability DBMS cluster, access to Kaspersky Security Center Web Console may be unavailable or significantly delayed. If Kaspersky Security Center Web Console remains inaccessible for more than 10 minutes, restart the IAM service by using the following command:

  ```
  systemctl restart kliam_srv.service
  ```

- 9157005, 9157085: When running the *Install required updates and fix vulnerabilities* task on a Windows managed device with the **Start installation at device restart or shutdown** option enabled, the task may fail with an error. This issue may occur when a large number of updates are scheduled for installation. To resolve the issue, run the task without enabling the **Start installation at device restart or shutdown** option.

- 9272534: If the table of users contains more than 50,000 users, only the first 50,000 users are displayed, and the remaining users are not shown.

- 9291235: After restoring a backup on Administration Server version 16.1, Kaspersky Security Center Web Console displays the sign-in page. After successful authentication, a one-time security code for two-factor authentication is requested. When a valid one-time security code is entered, an error message is displayed indicating that the one-time security code is incorrect. In this case, wait a few minutes and then manually refresh the page to retry signing in to Kaspersky Security Center Web Console. Once the backup restoration process has fully completed, authentication will be successful on the next attempt.

- 7939561: When attempting to modify a protected user account, clicking the **Cancel** button in the **Account protection** credential entry window results in an error.

- 8562938: Opening the port for mobile devices in the Administration Server policy properties does not enable the Mobile Device Management feature and does not trigger the generation of a mobile certificate. To enable the Mobile Device Management feature, the port for mobile devices must be opened in the Administration Server properties.

- 8732282: For a user who has the **User cannot change password** option enabled in account properties in Active Directory, the **Reset password** response action in Active Directory will not be executed. The domain controller administrator has to either disable the **User cannot change password** option for this user or manually reset the password. This issue occurs if you have the Kaspersky Next XDR Optimum license, integration with Active Directory is enabled, and the user is included in an Active Directory security group.

- 8688182: If the user has the **Password never expires** option enabled in account properties in Active Directory, then after executing the **Reset password** response action, the **Password never expires** option is disabled, and the user will be required to change their domain password at the next login. This issue occurs if you have the Kaspersky Next XDR Optimum license, integration with Active Directory is enabled, and the user is included in an Active Directory security group.

- 8703857: Proxy server connection for Kaspersky Security Center Web Console and management web plug-ins is established only if the proxy server supports basic-authentication.

- 7911778: When you run the **Uninstall application remotely** task to uninstall Network Agent from a device that is running an operating system with the Arm architecture and that also has an unsynchronized time with the Administration Server, the task status does not change from **Running** to **Completed**, even after Network Agent has been successfully uninstalled from the device. To resolve this issue, synchronize the time on the device with the installed Network Agent and the time on the device with the Administration Server before running the **Uninstall application remotely**.

- 6896585: A managed device cannot connect to KSN through the KSN Proxy service if Kaspersky Security Center Linux is installed on a device that has cyrillic symbols in its name.

- 7523299: Network Agent does not restart after killing its process on a managed device running CentOS 6.6.

- 7835858: If you create a task with the **Every N days** and **By days of week** scheduling settings in Kaspersky Security Center Web Console version 15.2 or later, and then open the task in earlier versions of Kaspersky Security Center Web Console or Administration Console (for example, when the task is also applied on the secondary Administration Servers which can be both Linux-based and Windows-based), the scheduling settings may be displayed incorrectly, or an error may occur.

- 7208621: When you import the *Download updates to the repositories of distribution points* or *Update verification* task the **Select devices to which the task will be assigned** option is enabled. These tasks cannot be assigned to a device selection or specific devices. If you assign the *Download updates to the repositories of distribution points* or *Update verification* task to specific devices, the task will be imported incorrectly.

- 6511063: If an application from the **Applications registry** section was detected on a Linux device, the application properties do not contain information about related executable files.

- 5915107: In reports with a letter format, a page break may cut a text line horizontally.

- 5556109: A managed device that has more than one network adapter sends Administration Server information about the MAC address of the network adapter that is not the one that is used to connect to Administration Server.

- 9093038: If Kaspersky Security Center Linux Administration Server does not start after installation and the operating system log contains error 213/SECUREBITS related to kladminserver_srv.service, execute the following commands as a superuser:

```
mkdir -p /etc/systemd/system/kladminserver_srv.service.d
echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kladminserver_srv.service.d/override.conf
mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/klwebsrv_srv.service.d/override.conf
```

If Kaspersky Security Center Web Console does not start after installation and the operating system log contains error 213/SECUREBITS related to KSCWebConsole.service, execute the following commands as a superuser:

```
mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
mkdir -p /etc/systemd/system/KSCWebConsole.service.d
echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsole.service.d/override.conf
```

If the kliam_srv service does not start after installation and the operating system log contains the 213/SECUREBITS error related to the service, execute the following commands as a superuser:

```
mkdir -p /etc/systemd/system/kliam_srv.service.d
echo "[Service]" > /etc/systemd/system/kliam_srv.service.d/override.conf
echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kliam_srv.service.d/override.conf
```

- 9165434: NTLM authentication does not work for user accounts within the Protected Users group.

# Contact Technical Support

This section describes how to get technical support and the terms on which it is available.

## How to get technical support

If you did not find a solution to your problem in the documentation or other sources of information about Kaspersky Security Center Linux, we recommend contacting Technical Support. Technical Support specialists will answer all your questions about installing and using Kaspersky Security Center.

Kaspersky provides support of Kaspersky Security Center during its lifecycle (see the application support lifecycle page). Before contacting Technical Support, please read the support rules.

You can contact Technical Support in one of the following ways:

- By visiting the Technical Support website
- By submitting a request to Kaspersky Technical Support from the Kaspersky CompanyAccount portal

## Technical support via Kaspersky CompanyAccount

Kaspersky CompanyAccount is a portal for companies that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky specialists through online requests. You can use Kaspersky CompanyAccount to track the status of your online requests as they are processed by Kaspersky experts and keep a history of such requests.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian

- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website.

# Obtaining dump files of Administration Server

Dump files of Administration Server contains all information about the Administration Server processes at a point in time. Dump files of Administration Server are stored in the /var/lib/systemd/coredump directory. Dump files are stored as long as Kaspersky Security Center Linux is in use, and are deleted permanently when the it is removed. Dump files are not sent to Kaspersky automatically.

If Administration Server crashes, you can contact Kaspersky Technical Support. A Technical Support specialist may ask you to send the dump files of Administration Server for further analysis at Kaspersky.

Dump files may contain personal data. We recommend protecting information from unauthorized access before sending it to Kaspersky.

# Sources of information about the application

## Kaspersky Security Center Linux page on the Kaspersky website

On the Kaspersky Security Center Linux page on the Kaspersky website, you can view general information about the application, its functions, and features.

## Kaspersky Security Center Linux page in the Knowledge Base

The *Knowledge Base* is a section on the Kaspersky Technical Support website.

On the Kaspersky Security Center Linux page in the Knowledge Base, you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to buy, install, and use the application.

Articles in the Knowledge Base may provide answers to questions that relate both to Kaspersky Security Center Linux as well as to other Kaspersky applications. Articles in the Knowledge Base may also contain Technical Support news.

## Discuss Kaspersky applications with the community

If your question does not require an immediate answer, you can discuss it with Kaspersky experts and other users on our Forum.

On the Forum, you can view discussion topics, post your comments, and create new discussion topics.

> An internet connection is required to access website resources.

If you cannot find a solution to your problem, contact Technical Support.

# Glossary

## Active key

A key that is currently used by the application.

## Administration Console

The Kaspersky Security Center Linux component that provides the user interface of the administrative services of the Administration Server and the Network Agent.

## Administration Group

A set of devices grouped by function and by installed Kaspersky applications. Devices are grouped as a single entity for the convenience of management. A group can include other groups. Group policies and group tasks can be created for each installed application in the group.

## Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky applications that are installed on the corporate network and controls such applications.

## Administration Server certificate

The certificate for authentication of the Administration Server is when the Administration Console connects to it and when communicating with client devices. The Administration Server certificate is created during installation of the Administration Server component and is stored in the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert folder on the Administration Server.

## Administration Server client (Client device)

A device, server, or workstation on which the Network Agent and managed Kaspersky applications are installed and running.

## Administrator rights

The level of the user's rights and privileges required for administration of Exchange objects within an Exchange organization.

## Administrator's workstation

The device on which the Administration Console is installed acts as the component that provides the management interface of Kaspersky Security Center Linux.

From the administrator's workstation, the administrator manages the server part of Kaspersky Security Center by building and controlling the centralized protection system of the organization's network based on Kaspersky applications.

## Anti-virus databases

Databases that contain information about computer security threats known to Kaspersky as of when the anti-virus databases are released. Entries in anti-virus databases allow malicious code to be detected in scanned objects. Anti-virus databases are created by Kaspersky specialists and updated hourly.

## Anti-virus protection service provider

An organization that provides a client organization with anti-virus protection services based on Kaspersky solutions.

## Anti-virus security of the network

A set of technical and organizational measures that lower the risk of allowing viruses and spam to penetrate the network of an organization, and that prevent network attacks, phishing, and other threats. The anti-virus security of the network increases when you use security applications and services and when you apply and adhere to the corporate data security policy.

## Application settings

Application settings that are common to all types of tasks and govern the overall operation of the application, such as application performance settings, report settings, and backup settings.

## Application Shop

Component of Kaspersky Security Center Linux. Application Shop is used for installing applications on Android devices owned by users. Application Shop allows you to publish the APK files of applications and links to applications in Google Play.

## Authentication Agent

Interface that lets you complete authentication to access encrypted hard drives and load the operating system after the bootable hard drive has been encrypted.

## Available update

A set of updates for Kaspersky application modules, including critical updates accumulated over a certain period of time and changes to the application's architecture.

## Backup copying of Administration Server data

Copying of the Administration Server data for backup and subsequent restoration performed by using the backup utility. The utility can save:

- The knowledge base of the Administration Server (policies, tasks, application settings, events saved on the Administration Server)
- Configuration information about the structure of administration groups and client devices
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates)
- Administration Server certificate

## Backup folder

Special folder for storage of Administration Server data copies created using the backup utility.

## Broadcast domain

A logical area of a network in which all nodes can exchange data using a broadcasting channel at the level of OSI (Open Systems Interconnection Basic Reference Model).

## Centralized application management

Remote application management using the administration services provided in Kaspersky Security Center.

## Client administrator

A staff member of a client organization who is responsible for monitoring the anti-virus security status.

## Cloud Discovery

Cloud Discovery manages user access to cloud services. Examples of cloud services are Microsoft Teams, Salesforce, Microsoft Office 365. Cloud services are grouped into categories, for example, *File sharing*, *Instant messaging*, *Email*.

## Configuration profile

Policy that contains a collection of settings and restrictions for an iOS MDM mobile device.

## Connection gateway

A *connection gateway* is a Network Agent acting in a special mode. A connection gateway accepts connections from other Network Agents and tunnels them to the Administration Server through its own connection with the Server. Unlike an ordinary Network Agent, a connection gateway waits for connections from the Administration Server rather than establishes connections to the Administration Server.

## Demilitarized zone (DMZ)

Demilitarized zone is a segment of a local network that contains servers, which respond to requests from the global Web. In order to ensure the security of an organization's local network, access to the LAN from the demilitarized zone is protected with a firewall.

## Device owner

Device owner is a user whom the administrator can contact when the need arises to perform certain operations on a device.

## Direct application management

Application management through a local interface.

## Event repository

A part of the Administration Server database dedicated to storage of information about events that occur in Kaspersky Security Center Linux.

## Event severity

Property of an event encountered during the operation of a Kaspersky application. There are four severity levels:

- Critical event
- Functional failures
- Warning
- Info

Events of the same type can have different severity levels depending on the situation in which the event occurred.

## FileTransferBridge

An internal component of Kaspersky Security Center Linux that provides local delivery of Kaspersky application updates. FileTransferBridge is integrated into Network Agent (klnagent) and runs locally on each managed device.

When Kaspersky applications receive updates from Kaspersky Security Center Linux, Network Agent downloads the update files from the Administration Server or a distribution point. FileTransferBridge then transfers the files locally to the installed Kaspersky applications, ensuring reliable delivery of database updates and software patches.

FileTransferBridge uses TCP ports 30522 and 30523. The ports listen only on the localhost interface (127.0.0.1) and do not accept incoming connections from external networks.

## Group task

A task defined for an administration group and performed on all client devices included in that administration group.

## Home Administration Server

Home Administration Server is the Administration Server that was specified during Network Agent installation. The home Administration Server can be used in settings of Network Agent connection profiles.

## HTTPS

Secure protocol for data transfer, using encryption, between a browser and a web server. HTTPS is used to gain access to restricted information, such as corporate or financial data.

## Identity and Access Manager (IAM)

A component of Administration Server that enables you to use domain authentication (single sign-on). The single sign-on feature allows a user to enable secure authentication in Kaspersky Security Center Web Console without having to re-enter the password on the corporate network.

## Incompatible application

An anti-virus application from a third-party developer or a Kaspersky application that does not support management through Kaspersky Security Center Linux.

## Installation package

A set of files created for remote installation of a Kaspersky application by using the Kaspersky Security Center remote administration system. The installation package contains a range of settings needed to install the application and get it running immediately after installation. Settings correspond to application defaults. The installation package is created using files with the .kpd and .kud extensions included in the application distribution kit.

## Internal users

The accounts of internal users are used to work with virtual Administration Servers. The administrator can use an internal user account to launch the Kaspersky Security Center Web Console and view information about the status of the anti-virus security status of the network. In Kaspersky Security Center Linux, internal users have the rights of real users.

The accounts of internal users are created and used only within Kaspersky Security Center Linux. No data on internal users is transferred to the operating system. Kaspersky Security Center Linux authenticates internal users.

## iOS MDM device

A mobile device that is connected to the iOS MDM Server by using the iOS MDM protocol. Devices running the iOS operating system can be connected and managed by means of the iOS MDM protocol.

## iOS MDM Server

A component of Kaspersky Security Center that is installed on a client device, allowing connection of iOS mobile devices to the Administration Server and management of iOS mobile devices through Apple Push Notifications (APNs).

## JavaScript

A programming language that expands the performance of web pages. Web pages created using JavaScript can perform functions (for example, change the view of interface elements or open additional windows) without refreshing the web page with new data from a web server. To view pages created by using JavaScript, enable JavaScript support in the configuration of your browser.

## Kaspersky Security Center Linux Administrator

The person managing application operations through the Kaspersky Security Center Linux remote centralized administration system.

## Kaspersky Security Center Linux Web Server

A component of Kaspersky Security Center Linux that is installed together with Administration Server. The Web Server is designed for transmission over a network of stand-alone installation packages, iOS MDM profiles, and files from a shared folder.

## Kaspersky Security Center Operator

A user who monitors the status and operation of a protection system managed with Kaspersky Security Center.

## Kaspersky Security Center System Health Validator (SHV)

A component of Kaspersky Security Center Linux designed for checking the operating system's operability in case of concurrent operation of Kaspersky Security Center Linux and Microsoft NAP.

## Kaspersky update servers

HTTP servers at Kaspersky from which Kaspersky applications download database and application module updates.

## Key file

A file in xxxxxxxx.key format that makes it possible to use a Kaspersky application under a trial or commercial license. You can use the application only if you have a key file.

## License term

The time period during which you are allowed to use the functionality of the application and additional services. The services you can use depend on the type of the license.

## Lightweight Nagent (LWNGT)

A protocol for interaction with Kaspersky Endpoint Security on mobile devices. The LWNGT (also called Mobile protocol) functions as Network Agent without actually installing Network Agent on mobile devices.

## Local installation

Installation of a protection application on a device on a corporate network that involves starting the installation manually from a distribution package of the protection application or manually running a published installation package that was pre-downloaded to the device.

## Local task

A task defined and running on a single client device.

## Managed devices

Corporate networked devices that are included in an administration group.

## Manual installation

Installation of a protection application on a device in the corporate network from a distribution package. Manual installation requires the involvement of an administrator or another IT specialist. Usually manual installation is done if remote installation has completed with an error.

## Network Agent

A Kaspersky Security Center Linux component that enables interaction between the Administration Server and Kaspersky applications that are installed on a specific network node (workstation or server). This component is common to all of the company's applications for Windows. There are separate versions of Network Agent for Kaspersky applications for Novell®, Unix™, and Mac.

## Network Location Awareness (NLA)

A Windows service that helps an operating system identify the current network. NLA detects network changes and adjusts the security configuration of the device.

## Network protection status

Current protection status, which defines the safety of corporate networked devices. The network protection status includes such factors as installed protection applications, usage of keys, and number and types of threats detected.

## Patch importance level

Attribute of the patch. There are five importance levels for Microsoft patches and third-party patches:

- Critical
- High
- Medium

- Low
- Unknown

The importance level of a third-party patch or Microsoft patch is determined by the least favorable severity level among the vulnerabilities that the patches should fix.

## Policy

A policy determines an application's settings and manages the ability to configure that application on computers within an administration group. An individual policy must be created for each application. You can create an unlimited number policies for applications installed on devices in each administration group, but only one policy can be applied at a time to each application within an administration group.

## Profile

Collection of settings of Exchange mobile devices that define their behavior when connected to a Microsoft Exchange Server.

## Protection status

Current protection status, which reflects the protection level of the device.

## Provisioning profile

Collection of settings for applications' operation on iOS mobile devices. A provisioning profile contains information about the license; it is linked to a specific application.

## Remote installation

Installation of Kaspersky applications by using the services provided by Kaspersky Security Center Linux.

## Reserve key

A key that certifies the right to use the application but is not currently being used.

## Restoration

Relocation of the original object from Quarantine or Backup to its original folder where the object had been stored before it was quarantined, disinfected or deleted, or to a user-defined folder.

## Restoration of Administration Server data

Restoration of Administration Server data from the information saved in Backup by using the backup utility. The utility can restore:

- The knowledge base of the Administration Server (policies, tasks, application settings, events saved on the Administration Server)
- Configuration information about the structure of administration groups and client devices
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates)
- Administration Server certificate

## Role group

A group of users of Exchange ActiveSync mobile devices who have been granted identical administrator rights.

## Service provider's administrator

A staff member at an anti-virus protection service provider. This administrator performs installation and maintenance jobs for anti-virus protection systems based on Kaspersky anti-virus products and also provides technical support to customers.

## Shared certificate

A certificate intended for identifying the user's mobile device.

## SSL

A data encryption protocol used on the internet and local networks. The Secure Sockets Layer (SSL) protocol is used in web applications to create a secure connection between a client and server.

## Task

Functions performed by the Kaspersky application are implemented as tasks, such as: Real-time file protection, Full computer scan, and Database update.

## Task for specific devices

A task assigned to a set of client devices from arbitrary administration groups and performed on those devices.

## Task settings

Application settings that are specific to each task type.

## Update Agent

Computer that has Network Agent installed and is used for update distribution, remote installation of applications, getting information about computers in an administration group and/or broadcasting domain. Distribution points are designed to reduce the load on the Administration Server during update distribution and to optimize network traffic. Distribution points can be assigned automatically, by the Administration Server, or manually, by the administrator.

## Updating

The procedure of replacing or adding new files (databases or software modules) retrieved from the Kaspersky update servers.

## Virtual Administration Server

A component of Kaspersky Security Center Linux, designed for management of the protection system of a client organization's network.

Virtual Administration Server is a particular case of a secondary Administration Server and has the following restrictions as compared with a physical Administration Server:

- Virtual Administration Server can be created only on a primary Administration Server.
- Virtual Administration Server uses the primary Administration Server database in its operation. Data backup and restoration tasks, as well as update scan and download tasks, are not supported on a virtual Administration Server.
- Virtual Server does not support creation of secondary Administration Servers (including virtual Servers).

## Virus outbreak

A series of deliberate attempts to infect a device with a virus.

## Vulnerability

A flaw in an operating system or an application that may be exploited by attackers to penetrate the operating system or application, and compromise its integrity. The presence of a large number of vulnerabilities in an operating system makes it unreliable, because malware that penetrate the operating system may cause disruptions in the operating system itself and in installed applications.

# Information about third-party code

Information about third-party code is contained in the file legal_notices.txt, in the application installation directory.

# Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Adobe, Acrobat, Flash, PostScript, and Shockwave are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

AMD, AMD64 are trademarks or registered trademarks of Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace are trademarks of Amazon.com, Inc. or its affiliates.

Apache is either a registered trademark or a trademark of the Apache Software Foundation in the United States and/or other countries.

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, and Touch ID are trademarks of Apple Inc.

Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Ubuntu, LTS are registered trademarks of Canonical Ltd. Cisco, Cisco Jabber, Cisco Systems, IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Citrix, XenServer are either registered trademarks or trademarks of Cloud Software Group, Inc., and/or its subsidiaries in the United States and/or other countries.

Corel is a trademark or registered trademark of Corel Corporation and/or its subsidiaries in Canada, the United States and/or other countries.

Cloudflare, the Cloudflare logo, and Cloudflare Workers are trademarks and/or registered trademarks of Cloudflare, Inc. in the United States and other jurisdictions.

Dropbox is a trademark of Dropbox, Inc.

Radmin is a registered trademark of Famatech.

Firebird is a registered trademark of the Firebird Foundation.

Foxit is a registered trademark of Foxit Corporation.

The FreeBSD mark is a registered trademark of The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Google Public DNS, Hangouts, and YouTube are trademarks of Google LLC.

EulerOS, FusionCompute, FusionSphere are trademarks of Huawei Technologies Co., Ltd.

Intel, Core, Xeon are trademarks of Intel Corporation or its subsidiaries.

IBM, QRadar are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Node.js is a trademark of Joyent, Inc.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Logitech is either a registered trademark or trademark of Logitech in the United States and/or other countries.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, Office 365, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista, and Windows Azure are trademarks of the Microsoft group of companies.

Mozilla, Firefox, Thunderbird are trademarks of the Mozilla Foundation in the U.S. and other countries.

Novell is a registered trademark of Novell Enterprises Inc. in the United States and other countries.

OpenSSL is a trademark owned by the OpenSSL Software Foundation.

OpenVPN is a registered trademark of OpenVPN, Inc.

Oracle, Java, JavaScript, and TouchDown are registered trademarks of Oracle and/or its affiliates.

Parallels, the Parallels logo, and Coherence are trademarks or registered trademarks of Parallels International GmbH.

Chef is a trademark or registered trademark of Progress Software Corporation and/or one of its subsidiaries or affiliates in the U.S. and/or other countries.

Puppet is a trademark or registered trademark of Puppet, Inc.

Python is a trademark or registered trademark of the Python Software Foundation.

Red Hat, Fedora, and Red Hat Enterprise Linux are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Ansible is a registered trademark of Red Hat, Inc. in the United States and other countries.

CentOS is a trademark or registered trademark of Red Hat, Inc. or its subsidiaries in the United States and other countries.

The BlackBerry trademark is owned by Research In Motion Limited and is registered in the United States and may be pending registration or registered in other countries.

Rocky Linux is a trademark of The Rocky Enterprise Software Foundation.

Samsung is a trademark of SAMSUNG in the United States or other countries.

Debian is a registered trademark of Software in the Public Interest, Inc.

Splunk, SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries.

SUSE is a registered trademark of SUSE LLC in the United States and other countries.

Symbian trademark is owned by the Symbian Foundation Ltd.

OpenAPI is a trademark of The Linux Foundation.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Zabbix is a registered trademark of Zabbix SIA.