kaspersky

Kaspersky Next Expert View

© 2026 AO Kaspersky Lab

Contents

Kaspersky Next Expert View Help

What's new

Fixed issues

Kaspersky Next Expert View

- Hardware and software requirements for Kaspersky Next Expert View
- Compatible Kaspersky applications and solutions
- Localization of Kaspersky Next Expert View
- Comparison of Kaspersky Security Center and Kaspersky Next Expert View

Architecture and basic concepts

- Architecture
- Ports used by Kaspersky Next Expert View
- Basic concepts
  - Network Agent
  - Administration groups
  - Hierarchy of Administration Servers
  - Virtual Administration Server
  - Distribution point
  - Management web plug-in
  - Policies
  - Policy profiles
  - How local application settings relate to policies

Application licensing

- Licensing of Kaspersky Next Expert View
- About the trial mode of Kaspersky Next Expert View
- Using Kaspersky Marketplace to choose Kaspersky business solutions
- Licenses and the minimum number of devices for each license
- Events of the license limit exceeded
- Methods of distribution of the activation codes to the managed devices
- Adding an Administration Server license key
- 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 in the Administration Server repository
- Viewing information about the license keys used for a specific Kaspersky application
- Removing an Administration Server license key
- Deleting a license key from the repository
- Viewing the list of devices where a Kaspersky application is not activated
- Revoking consent with an End User License Agreement
- Renewing licenses for Kaspersky applications
- Use of Kaspersky Next Expert View after the license expiration
- Licensing definitions
  - About the license
  - About the License Certificate

- About the license key
- About the activation code
- About the subscription

Data provision
- Data sent to Kaspersky servers
- Data necessary for the functioning of managed applications
- User data processed locally
- About legal documents of Kaspersky Next Expert View

Hardening Guide
- Administration Server deployment
- Accounts and authentication
- Managing protection of client devices
- Configuring protection for managed applications
- Event transfer to third-party systems
- Security recommendations for third-party information systems
- Recommendations for using Kaspersky security applications

Interface of Kaspersky Next Expert View
- Changing the language of the Kaspersky Next Expert View interface
- Changing the Kaspersky Next Expert View home page
- Pinning and unpinning sections of the main menu
- Returning to the list of workspaces

Initial configuration of Kaspersky Next Expert View

Scenario: Creating a hierarchy of Administration Servers managed through Kaspersky Next Expert View

Migration to Kaspersky Next Expert View
- Methods of migration to Kaspersky Next Expert View
- Scenario: Migration without a hierarchy of Administration Servers
- Migration wizard
  - Step 1. Exporting managed devices, objects, and settings from Kaspersky Security Center Web Console
  - Step 2. Importing the export file to Kaspersky Next Expert View
  - Step 3. Re-installing Network Agent on devices managed through Kaspersky Next Expert View
- Migration with a hierarchy of Administration Servers
- Scenario: Migration of devices running Linux or macOS operating systems
- Scenario: Reverse migration from Kaspersky Next Expert View to Kaspersky Security Center
- Migration with virtual Administration Servers
  - Scenario: Migration with virtual Administration Servers by moving devices
  - Scenario: Manual migration with virtual Administration Servers
  - Scenario: Moving devices from administration groups under management of virtual Servers

Quick start wizard
- About quick start wizard
- Starting quick start wizard
- Step 1. Selecting installation packages to download
- Step 2. Configuring a proxy server
- Step 3. Configuring Kaspersky Security Network
- Step 4. Configuring third-party update management
- Step 5. Creating a basic network protection configuration
- Step 6. Closing the quick start wizard

Kaspersky applications initial deployment
Scenario: Kaspersky applications initial deployment
Creating installation packages for Kaspersky applications
Distributing installation packages to secondary Administration Servers
Creating a stand-alone installation packages for Network Agent
Viewing the list of stand-alone installation packages
Creating custom installation packages
Requirements for a distribution point
Network Agent installation package settings
Virtual infrastructure
Tips on reducing the load on virtual machines
Support of dynamic virtual machines
Support of virtual machines copying
Usage of Network Agent for Windows, Linux, and macOS: Comparison
Specifying settings for remote installation on Unix devices
Replacing third-party security applications
Options for manual installation of applications
Forced deployment through the remote installation task of Kaspersky Next Expert View
Protection deployment wizard
Step 1. Starting Protection deployment wizard
Step 2. Selecting the installation package
Step 3. Selecting Network Agent version
Step 4. Selecting devices
Step 5. Specifying the remote installation task settings
Step 6. Restart management
Step 7. Removing incompatible applications before installation
Step 8. Moving devices to Managed devices
Step 9. Selecting accounts to access devices
Step 10. Starting installation
Network settings for interaction with external services
Preparing a device running Astra Linux in the closed software environment mode for installation of Network Agent
Preparing a Linux device and installing Network Agent on a Linux device remotely
Installing applications using a remote installation task
Installing an application remotely
Installing applications on secondary Administration Servers
Starting and stopping Kaspersky applications
Mobile Device Management
Detection and response capabilities
Data Discovery
About Data Discovery
Categories of information detected by Data Discovery
Starting the use of Data Discovery
Accepting the terms and conditions of the Data Discovery Agreement
Connecting a Microsoft 365 organization to your workspace
Viewing information about Data Discovery detections
Example of analyzing a Data Discovery detection

Exporting information about Data Discovery detections
Disabling Data Discovery
Discovering networked devices and creating administration groups
Scenario: Discovering networked devices
Network polling
Windows network polling
Domain controller polling
IP range polling
Configuring a Samba domain controller
Adding and modifying an IP range
Adjustment of distribution points and connection gateways
Calculating the number and configuration of distribution points
Standard configuration of distribution points: Single office
Standard configuration of distribution points: Multiple small remote offices
Assigning distribution points manually
Modifying the list of distribution points for an administration group
Using a distribution point as a push server
Using the "Do not disconnect from the Administration Server" option to provide continuous connectivity between a managed device and the Administration Server
Creating administration groups
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
Configuring retention rules for unassigned devices
Equipment inventory
Adding information about new devices
Configuring criteria used to define enterprise devices
Configuring network protection
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
Network Agent policy settings
Comparison of Network Agent policy settings by operating systems
Configuring protection settings of managed applications
Manual setup of the group update task for Kaspersky Endpoint Security
Tasks
About tasks
About task scope
Creating a task
Viewing the task list
Starting a task manually
Starting a task for selected devices
General task settings and properties
Exporting a task

- Importing a task
- Viewing task run results stored on the Administration Server

Managing client devices

- Settings of a managed device
- Manually checking the connection between a client device and the Administration Server. klnagchk utility
- 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
- Viewing and configuring the actions when devices show inactivity
- About device statuses
- Configuring the switching of device statuses
- Changing the Administration Server for client devices
- Avoiding conflicts between multiple Administration Servers
- Creating Administration Server connection profiles
- About clusters and server arrays
- Properties of a cluster or server array
- 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 devices manually
  - Removing assigned tags from devices
  - 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
- Quarantine and File backups
  - Downloading a file from repositories
  - Deleting files from repositories
- 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 an application and downloading the results

- Running an application on a client device
- Generating a dump file for an application
- Remotely connecting to the desktop of a client device
- Connecting to devices through Windows Desktop Sharing
- Triggering of rules in Smart Training mode
- Viewing the list of detections performed using Adaptive Anomaly Control rules
- Adding exclusions from the Adaptive Anomaly Control rules

Managing administration groups
- Creating administration groups
- Automatic installation of applications on devices in an administration group
- Moving administration groups
- Deleting administration groups

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
- Modifying a policy
- General policy settings
- Enabling and disabling a policy inheritance option
- Copying a policy
- Moving a policy
- Exporting a policy
- Importing a policy
- Viewing the policy distribution status chart
- Activating a policy automatically at the Virus outbreak event
- Forced synchronization
- Deleting a policy
- Managing policy profiles
- Viewing the profiles of a policy
- Changing a policy profile priority
- Creating a policy profile
- Modifying a policy profile
- Copying a policy profile
- Creating a policy profile activation rule
- Deleting a policy profile
- Exporting and importing a policy profile

Data encryption and protection
- Viewing the list of encrypted drives
- Creating and viewing encryption reports
- Granting access to an encrypted drive in offline mode

- Users and user roles
  - About user accounts
  - Adding an account of an internal user
  - Deleting an account of an internal user
  - Assigning workspace administrators
  - 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
  - Assigning a role to a user or a security group
  - Creating a user role
  - Editing a user role
  - Editing the scope of a user role
  - Deleting a user role
  - Associating policy profiles with roles
  - Creating a security group
  - Editing a security group
  - Adding user accounts to an internal group
  - Deleting a security group
  - Configuring ADFS integration
  - Configuring integration with Microsoft Entra ID
    - Enabling Microsoft Entra ID polling
    - Adding Kaspersky Next Expert View to the list of applications
  - Assigning a user as a device owner
  - Assigning a user as a Linux device owner after installation of Network Agent
- Managing object revisions
  - Adding a revision description
  - Rolling back an object to a previous revision
  - Viewing and saving a policy revision
  - Comparing policy revisions
- Kaspersky Security Network (KSN)
  - About KSN
  - Enabling and disabling KSN
  - Viewing the accepted KSN Statement
  - Accepting an updated KSN Statement
  - Checking whether the distribution point works as KSN proxy server
- Deletion of objects

Updating Kaspersky databases and applications

- Scenario: Regular updating Kaspersky databases and applications
- About updating Kaspersky databases, software modules, and applications
- Creating the task for downloading updates to the repositories of distribution points
- Configuring managed devices to receive updates only from distribution points
- Enabling and disabling automatic updating and patching for Kaspersky Next Expert View components
- Automatic installation of updates for Kaspersky Endpoint Security for Windows
- About update statuses

Approving and declining software updates
Using diff files for updating Kaspersky databases and software modules
Updating Kaspersky databases and software modules on offline devices
Managing third-party applications on client devices
Limitations of Vulnerability and patch management
Availability of Vulnerability and patch management features in trial and commercial mode and under various licensing options
About third-party applications
Third-party software updates
Scenario: Updating third-party software
Installing third-party software updates
Creating the Find vulnerabilities and required updates task
Find vulnerabilities and required updates task settings
Creating the Install required updates and fix vulnerabilities task
Adding rules for update installation
Creating the Install Windows Update 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
Updating third-party applications automatically
Finding and fixing software vulnerabilities
Fixing software vulnerabilities
Creating the Fix vulnerabilities task
Creating the Install required updates and fix vulnerabilities task
Adding rules for update installation
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
Scenario: Finding and fixing software vulnerabilities
Setting the maximum storage period for the information about fixed vulnerabilities
Managing applications run on client devices
Using Application Control to manage executable files
Application Control modes and categories
Obtaining and viewing a list of applications installed on client devices
Obtaining and viewing a list of executable files installed on client devices
Creating an application category with content added manually
Creating an application category that includes executable files from selected devices
Viewing the list of application categories
Configuring Application Control in the Kaspersky Endpoint Security for Windows policy
Adding event-related executable files to the application category
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
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
Configuring Administration Server
Hierarchy of Administration Servers
Creating a hierarchy of Administration Servers: adding a secondary Administration Server
Configuring storage term of events concerning to the deleted devices
Aggregate emails about events
Limitations on management of secondary Administration Servers running on-premises through Kaspersky Next Expert View
Viewing the list of secondary Administration Servers
Deleting a hierarchy of Administration Servers
Configuring the interface
Managing virtual Administration Servers
Creating a virtual Administration Server
Enabling and disabling a virtual Administration Server
Assigning an administrator for a virtual Administration Server
Deleting a virtual Administration Server
Monitoring and reporting
Scenario: Monitoring and reporting
About types of monitoring and reporting
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
Events and event selections
About events in Kaspersky Next Expert View
Events of Kaspersky Next Expert View 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
Logging information about events for tasks and policies
Deleting events
Deleting event selections
Blocking frequent events
About blocking frequent events
Managing frequent events blocking
Removing blocking of frequent events
Notifications and device statuses
About notifications
Viewing attention-required notifications
Viewing system notifications
Viewing announcements
Disabling announcements
Configuring the switching of device statuses
Configuring notification delivery
Receiving license expiration warning
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
Active threats
Disinfecting an unprocessed file
Downloading an unprocessed file
Deleting files from the Active threats section
Working with Kaspersky Next Expert View 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

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 an application and downloading the results
Running an application on a client device
Generating a dump file for an application
Running remote diagnostics on a Linux-based client device
Export of events to SIEM systems
Configuring event export to SIEM systems
Before you begin
About event export
Configuring an event export in a SIEM system
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 Next Expert View for export of events to a SIEM system
Viewing export results
Quick Start Guide for Managed Service Providers (MSPs)
About Kaspersky Next Expert View
Key features of Kaspersky Next Expert View
About licensing of Kaspersky Next Expert View for MSPs
About detection and response capabilities for MSPs
Getting started with Kaspersky Next Expert View
Recommendations on managing your customers' devices
Typical deployment scheme for MSPs
Scenario: Protection deployment (tenant management through virtual Administration Servers)
Scenario: Protection deployment (tenant management through administration groups)
Joint usage of Kaspersky Security Center on-premises and Kaspersky Next Expert View
Licensing of Kaspersky applications for MSPs
Monitoring and reporting capabilities for MSPs
Working with Kaspersky Next Expert View in a cloud environment
Licensing options in a cloud environment
Preparing for work in a cloud environment through Kaspersky Next Expert View
Working in Amazon Web Services cloud environment
About work in Amazon Web Services cloud environment
Creating IAM user accounts for Amazon EC2 instances
Ensuring that Kaspersky Next Expert View has the permissions to work with AWS
Creating an IAM user account for work with Kaspersky Next Expert View

Working in Microsoft Azure cloud environment
About work in Microsoft Azure
Creating a subscription, Application ID, and password
Assigning a role to the Azure Application ID
Working in Google Cloud
Cloud environment configuration wizard in Kaspersky Next Expert View
Step 1. Checking the required plug-ins and installation packages
Step 2. Selecting the application activation method
Step 3. Selecting the cloud environment and authorization
Step 4. Segment polling and configuring synchronization with Cloud
Step 5. Configuring Kaspersky Security Network for Kaspersky Next Expert View
Step 6. Creating an initial configuration of protection
Network segment polling via Kaspersky Next Expert View
Adding connections for cloud segment polling via Kaspersky Next Expert View
Deleting a connection for cloud segment polling
Configuring the polling schedule via Kaspersky Next Expert View
Viewing the results of cloud segment polling via Kaspersky Next Expert View
Viewing the properties of cloud devices via Kaspersky Next Expert View
Synchronization with Cloud: Configuring the moving rule
Remote installation of applications to the Azure virtual machines
Contact Technical Support
How to get technical support
Technical support via Kaspersky CompanyAccount
Information required for Kaspersky Technical Support specialists
Sources of information about the application
Known issues and limitations
Glossary
Active key
Administration Group
Administration Server
Amazon EC2 instance
AMI
Anti-virus databases
Anti-virus security of the network
Application settings
Application tag
Authentication Agent
Available update
AWS Application Program Interface (AWS API)
AWS Console
AWS IAM access key
Broadcast domain
Centralized application management
Cloud Discovery
Connection gateway
Demilitarized zone (DMZ)
Device owner

Device tag
Direct application management
Event repository
Event severity
Forced installation
Group task
Home Administration Server
HTTPS
IAM role
IAM user
Identity and Access Management (IAM)
Incompatible application
Installation package
JavaScript
Kaspersky Next Expert View
Kaspersky Next Expert View account
Kaspersky Next Expert View Administrator
Kaspersky Next Expert View Operator
Kaspersky Security Network (KSN)
Kaspersky update servers
Key file
License term
Lightweight Nagent (LWNGT)
Local installation
Local task
Managed device
Management web plug-in
Network Agent
Network Location Awareness (NLA)
Network protection status
Patch importance level
Policy
Policy profile
Protection status
Push server
Quarantine
Remote installation
Reserve key
Restoration
SSL
Task
Task for specific devices
Task settings
UEFI protection device
Update Agent
Updating
Virtual Administration Server

Virus activity threshold
Virus outbreak
Vulnerability
Work area
Information about third-party code
Trademark notices

Kaspersky Next Expert View Help

	**What's new** Find out what's new in the latest application release.		**Configuring network protection** Manage the security of an organization by configuring Kaspersky application policies and tasks in accordance with the organization's requirements.
	**Hardware and software requirements** Check which operating systems and application versions are supported.		**Kaspersky applications: regular updating databases and software modules** Maintain the reliability of the protection system.
	**Licensing of Kaspersky Next Expert View** Learn details about Kaspersky Next Expert View working in trial mode and in the commercial mode.		**Monitoring and reporting** View your infrastructure, protection statuses of networked devices, and statistics to manage the current protection state of your organization. You can also use reports.
	**Initial configuration** Start working with your workspace, configure Kaspersky Next Expert View according to your needs.		**Vulnerability and patch management** Find and fix vulnerabilities in third-party software.
	**Migration to Kaspersky Next Expert View** Migrate your existing administration groups and related objects from Kaspersky Security Center on-premises to Kaspersky Next Expert View.		**Export of events to SIEM systems** Configure exporting events to SIEM systems using the Syslog protocol.
	**Discovering networked devices** Discover the existing and new devices on your organization's network.		**Working in a cloud environment** Protect virtual machines in cloud environments: Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.
	**Adjustment of distribution points and/or connection gateways** Configure distribution points.		**Using the Kaspersky Next XDR Optimum functionality in Kaspersky Next Expert View** Configure integrations for responding to alerts and aggregate alerts belonging to the same incident to make the investigation process easier.
	**Kaspersky applications: centralized deployment** Kaspersky Lab software deployment		**Quick Start Guide for Managed Service Providers (MSPs)** Learn how to work with Kaspersky Next Expert View, if you are an administrator of MSP.

What's new

Update August, 2026

This update of Kaspersky Next Expert View includes the following improvements:

- Notification center is now available. Notification center displays notifications and announcements that help you stay aware of relevant events, changes, and recommendations related to your Administration Server and managed devices. You can search, sort, and filter notifications in the table. All unread notifications are also available by clicking the Notification icon ( ) next to the menu of your account.
- The **New custom installation package** window is modified. The window now includes a file uploader, and when the custom installation package size exceeds the limit, the system displays an error message.
- Kaspersky Next Expert View now supports work with:
  - Kaspersky Endpoint Security 14.1 for Windows.
  - Kaspersky Endpoint Security 12.5 for Linux

Update June, 2026

This update of Kaspersky Next Expert View includes the following improvements:

- You can now assign administrators to multiple virtual servers at once.
- You can now switch workspaces from trial to commercial mode. After switching, the workspace will not be deleted when the 30-day period expires.
- You can now add new users to your workspace in the Users & roles section. You can also assign new users as workspace administrators.
- Added the list of data processed by Kaspersky Next when connecting devices.
- Usability improvements:
  - Improved the distribution point assigning process: the list now displays only unassigned distribution points.
  - The algorithm for discovering networked devices has been improved. 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.

- Improved the **Console navigation** section's layout for more effective use of screen space.
- Improved the notification display readability across various system scenarios.

- Kaspersky Next Expert View supports work with:
  - Kaspersky Endpoint Security 14.0 for Windows.
  - Kaspersky Embedded Systems Security 4.0 for Linux.
  - Data Discovery: Detect more types of sensitive data and prevent sharing of critical or personal information.
  - iOS MDM Server: Connect iOS mobile devices to the Administration Server and manage it through Apple Push Notifications (APNs).

Update February, 2026

This update of Kaspersky Next Expert View includes the following improvements:

- 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 Next Expert View: the default number of displayed items has been increased to 50, and the custom number of displayed items is now preserved between sessions.
- Kaspersky Next Expert View supports work with the following Kaspersky applications:
  - Kaspersky Endpoint Security 12.12 for Windows.
  - Kaspersky Endpoint Security 12.4 for Linux
- Network Agent now supports work with the following new operating system versions:
  - CentOS Stream 10 64-bit
  - Debian GNU/Linux 13 (Trixie) 64-bit
  - Red Hat Enterprise Linux Server 10.x 64-bit
- Kaspersky Next Expert View infrastructure now supports the Kaspersky Next XDR Ultimate licenses.
- You can now take cybersecurity training that helps you become a professional in IT security.

Update October, 2025

This update of Kaspersky Next Expert View includes the following improvements:

- FreeIPA and ALD Pro domain controllers are supported.
- 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 **Assets (Devices)**.
    - **Quick links** is renamed to **Console navigation**.
  - You can minimize the main menu to icons, if necessary.
- 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 Next Expert View now supports work with:
  - Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit
  - The following Kaspersky applications:
    - Kaspersky Endpoint Security 12.11 for Windows.
    - Kaspersky Embedded Systems Security 4.0 for Windows

Update September, 2025

This update of Kaspersky Next Expert View includes the following improvements:

- 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.
- We have got rid of the "companies" notion, only "workspaces" are left. Therefore, your existing workspaces have been renamed to the following format: `[<company_name>]<workspace_name>`.

- Kaspersky Next Expert View infrastructure now contains a separate **Licenses** tab. If a license is used in multiple workspaces, you can view the total usage of the license on the **Licenses** tab.
- From the new **Licenses** tab, you can also view the actual legal documents for software solutions and security applications that are available on Kaspersky Next Expert View.
- By using special widgets and banners in Kaspersky Next Expert View infrastructure, managed service provider (MSP) administrators now have a bird's-eye view of the main health indicators across all their workspaces.

Update July, 2025

This update of Kaspersky Next Expert View includes the following 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.
- Some versions of Network Agent are no longer supported. Refer to the Application Support Lifecycle webpage and, if necessary, upgrade your Network Agent to the up-to-date version with the **Full support** or **Limited support** status.
- The **Scan** button is deleted from the **Quarantine** **section**.
- Kaspersky Next Expert View now supports the following Kaspersky applications:
  - Kaspersky Endpoint Security 12.10 for Windows.
  - Kaspersky Endpoint Security 12.3 for Linux
  - Kaspersky Endpoint Security 12.2 for Mac
- The user interface for workspace creation and management has been improved.

Update April, 2025

This update of Kaspersky Next Expert View includes the following improvements:

- Kaspersky Next Expert View now supports the following Kaspersky applications:
  - Kaspersky Embedded Systems Security 3.4 for Linux.
  - Kaspersky Endpoint Security 12.2 for Linux
  - Kaspersky Endpoint Security 12.8 for Windows.

- Upload and run an application (or script) for diagnostics on a managed device. You can now upload either the folder or archive containing the executable file, or the executable file itself. After the application is successfully executed, you can download the execution results.
- 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.
- New language support: Kaspersky Next Expert View infrastructure is available in the Chinese Simplified language.
- User experience improvements:
  - Available installation packages are displayed on one tab.
  - You can change the home page settings via the new **Quick links** section. By default, the **Home page settings** tab of the **Quick links** section is set as the home page.
  - Navigation through the administration groups is updated: you can go to the required subgroup by clicking the link with its name in the path to the administration group.
  - The **Pinned** section of the main menu is now called **Bookmarks**. You can add sections of Kaspersky Next Expert View to bookmarks, to access them quickly.

Update February, 2025

This update of Kaspersky Next Expert View improves performance when opening and navigating the Web Console.

Update October, 2024

This update of Kaspersky Next Expert View includes the following improvements:

- We have improved the integration with Microsoft Entra ID. Now, when a user signs out of the Microsoft Entra ID account that was used for authentication in Kaspersky Next Expert View, the session also ends for Kaspersky Next Expert View and the user is automatically signed out of the console.
- You can now view and download policy revisions. Kaspersky Next Expert View allows you to view a report in the HTML format or save the revision to a JSON file.
- Kaspersky Next Expert View now displays the latest task status known to the Administration Server.
- The **Report on network attacks** now includes the MAC address and port of the attacking machine.
- You can now close the right panel by clicking any place outside the panel. If you make any changes to the panel and then try to close it by clicking outside the panel, a confirmation window appears.
- The table header now stays pinned at the top when you scroll the table.

Update September, 2024

This update of Kaspersky Next Expert View includes the following improvements:

- Kaspersky Endpoint Agent 4.0 is supported.
- A number of old browser versions are no longer supported (Chrome earlier than version 128, Edge earlier than version 128, Firefox ESR earlier than version 115, Safari earlier than version 17.6).

Update April, 2024

This update of Kaspersky Next Expert View includes the following new features and improvements:

- A new Cloud Discovery feature. This feature 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.
- Integration with Microsoft Entra ID to allow the users in your organization to sign in to Kaspersky Next Expert View with their Microsoft Entra ID account credentials. Note, this feature is not available in the Russian Federation.
- You can now create connection profiles for connecting Network Agent to Administration Server. The connection profiles allow out-of-office users of laptops to change the method of connecting to an Administration Server or to switch between Administration Servers, depending on the current location of the device on the enterprise network.
- You can now open the list of your workspaces right from the main menu of the application.
- Two new localization languages were added—Traditional Chinese and Simplified Chinese.
- The default event storage setting in the task settings was changed from **Save all events** to **Save only task execution results**. This option reduces space consumption in the workspace database. The change affects only tasks created for Kaspersky Security Center. This setting remains without modification in the tasks for Kaspersky security applications.
- Kaspersky Next Expert View now additionally notifies you about the planned deletion of your workspace, 7 and 30 days after the last license key is deleted from the workspace or expires. This will give you more time to purchase another license and add its license key to the workspace.
- Kaspersky Business Hub and Kaspersky Next Expert View infrastructure now support the Kaspersky Next licenses. The application logo is changed automatically in accordance with the license that you use.
- Kaspersky Next Expert View now supports the following Kaspersky applications:
  - Kaspersky Endpoint Security for Windows version 12.4
  - Kaspersky Endpoint Security 12.0 for Mac Patch A
- When you migrate from one Kaspersky security application to another and the current application is password-protected, you can specify the uninstallation password right in the remote installation task properties.

- You can now customize the main menu of the application by pinning or unpinning your favorite menu sections. The pinned sections are added to the **Pinned** area for quick access.
- Optimized application interface and user experience when you select the **On completing another task** option while scheduling a task.
- The report on hardware now can include information about macOS devices.
- You can now select one or more client devices in the list of devices, and then launch a previously created task for them.

Update February, 2024

This update of Kaspersky Next Expert View includes the following new features and improvements:

- From the managed devices list, you can now select a device or several devices, and then assign an existing task to run on the selected devices. The current device scope of the task will be replaced with the devices that you selected.
- You can now assign device tags to multiple devices or remove device tags from multiple devices at once. From the managed devices list, select the devices, and then specify which tags you want to assign to or remove from the selected devices.
- Optimized appearance and user experience of the managed devices list. Added a new column **Tags** and the ability to filter devices by device tags.

Update January, 2024

Kaspersky Next Expert View now supports Kaspersky Endpoint Security 12.4 for Windows.

Update December, 2023

This update of Kaspersky Next Expert View includes the following new features and improvements:

- You can now check the connection to a SIEM system.
- Kaspersky Next Expert View now supports polling of a Microsoft Active Directory domain controller and a Samba domain controller through a Linux-based distribution point.
- Remote diagnostics of Linux-based managed devices.
- Kaspersky Next Expert View now supports the following Kaspersky applications:
  - Kaspersky Endpoint Security for Windows version 12.3 Patch A
  - Kaspersky Endpoint Security 12.0 for Linux

  - Kaspersky Endpoint Security 12.0 for Mac
  - Kaspersky Endpoint Agent 3.16
  - Kaspersky Embedded Systems Security 3.3 for Windows
- Two interface sections were hidden from the main menu as out of the scope of application functionality:
  - Encryption events (**Operations** → **Data encryption and protection** → **Encryption events**)
  - IP ranges (**Discovery & deployment** → **Discovery** → **IP ranges**)
- We have updated the text of the Data Processing Agreement for Kaspersky Next Expert View.
- A number of old browser versions are no longer supported (Firefox ESR earlier than version 102).

Update September, 2023

This update of Kaspersky Next Expert View includes the following new features and improvements:

- Kaspersky Next Expert View now supports Kaspersky Embedded Systems Security 3.3 for Linux.
- Kaspersky Next Expert View now supports Kaspersky Endpoint Security 12.2 for Windows.
- Optimization of user interface when working with the user list in the **Asset management** section.

Update June, 2023

This update of Kaspersky Next Expert View includes the following new features and improvements:

- A new Hardening Guide was released. We highly recommend that you carefully read the guide and follow the security recommendations for configuring Kaspersky Next Expert View and your network infrastructure.
- Kaspersky Next Expert View now supports Kaspersky Endpoint Security 11.3 for Mac.
- Kaspersky Next Expert View now supports Kaspersky Endpoint Security 11.4 for Linux.
- You can use Kaspersky Next Expert View to export event selections to a file, and then import the event selections to Kaspersky Security Center Windows or Kaspersky Security Center Linux.
- You can now use a distribution point as a push server for the devices managed by Network Agent. This feature allows you to make sure that continuous connectivity between a managed device and the Administration Server is established.
- Reorganization of the section with settings to integrate Kaspersky Next Expert View with other Kaspersky applications.
- Reorganization of the user interface of the **Remote diagnostics** section.

- You can now save information about all devices included in a device selection to a CSV file at once.
- A number of improvements in the user interface and usability, including the ability to select all items in a table.

Update March, 2023

This update of Kaspersky Next Expert View includes the following new features and improvements:

- Kaspersky Next Expert View now supports clusters and server arrays as managed devices. If a Kaspersky application is installed on a cluster node, Network Agent sends this information to Administration Server. In Web Console, clusters and server arrays are listed separately from other managed devices. You manage each cluster or server array as an individual, inseparable object.
- Kaspersky Next Expert View now supports Kaspersky Endpoint Security 12.0 for Windows.
- The maximum number of entries that a report can include was increased up to 2500 for a report in Web Console and up to 10,000 for a report that you export to a file.
- You can now choose whether or not you want to include the managed devices with the *OK* status in the Protection status report.
- You can now activate Kaspersky Next Expert View by using one of the following licenses or add the license keys of the listed licenses to an existing workspace:
  - Kaspersky Symphony Security
  - Kaspersky Symphony EDR
  - Kaspersky Symphony MDR
  - Kaspersky Next XDR Expert
- A special edition of Network Agent for Windows XP was released.
- The updated Network Agent for Linux supports the KSN Proxy service. Along with Windows-based distribution points, you can now use Linux-based distribution points to forward Kaspersky Security Network (KSN) requests from the managed devices. This feature allows you to redistribute and optimize traffic on the network.
- The updated Network Agent for Linux supports the Applications registry feature. Network Agent can compile a list of applications installed on a Linux-based managed device, and then transmit this list to Administration Server.
- You can use Kaspersky Next Expert View 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.

Update November, 2022

This update of Kaspersky Next Expert View includes the following new features and improvements:

- Kaspersky Next Expert View now supports Kaspersky Endpoint Security 11.3 for Linux.
- Kaspersky Next Expert View now supports Kaspersky Managed Detection and Response 2.1.18.
- Kaspersky Next Expert View now supports updated versions of Kaspersky Endpoint Security for Mac 11.2 and 11.2.1, to support macOS 13.
- Videos in the **Tutorials** section have been updated.

Update October, 2022

This update of Kaspersky Next Expert View includes the following new features and improvements:

- We have updated the text of the Data Processing Agreement for Kaspersky Next Expert View.
- Kaspersky Next Expert View infrastructure now notifies you about a workspace that has no active license key and that may be deleted if you do not add a new license key.
- Kaspersky Next Expert View now supports Kaspersky Endpoint Security 11.11.0 for Windows.
- Kaspersky Next Expert View now supports Kaspersky Endpoint Detection and Response Optimum 2.3.
- Kaspersky Embedded Systems Security 3.2 for Windows is supported.

Update September, 2022

This update of Kaspersky Next Expert View includes the following new features and improvements:

- You can now assign dedicated administrators for virtual Administration Servers. You create a user account for an administrator, and then grant the administrator the access rights to a virtual Administration Server. The assigned administrator has access only to the selected virtual Administration Server and cannot connect to the primary Administration Server or other secondary Administration Servers, physical or virtual.
- Optimized user experience when you delete a license key for Kaspersky Next Expert View. The new mechanism prevents you from deleting your last active license key by accident.
- You can now use Linux-based distribution points to download anti-virus databases for Kaspersky security applications through the *Download updates to the repositories of distribution points* task.
- Network Agent is now available in Japanese localization.
- In the Kaspersky Next Expert View interface, the all uppercase style of the section names has been changed to sentence-style capitalization.

Update August, 2022

New language support: Kaspersky Next Expert View is fully available in the Japanese language.

Update July, 2022

This update of Kaspersky Next Expert View includes the following new features and improvements:

- New versions of supported Kaspersky applications:
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 for Mac
  - Kaspersky Security for iOS 1.0.0
  - Kaspersky Endpoint Security 11.10.0 for Windows
- We have updated the text of the Agreement and Data Processing Agreement for Kaspersky Next Expert View.
- New language support: Kaspersky Next Expert View infrastructure is now available in Japanese. The support of the Japanese language inside Kaspersky Next Expert View workspaces is coming soon.

Update April, 2022

This update of Kaspersky Next Expert View includes the following new features and improvements:

- Kaspersky Next Expert View now supports Kaspersky Endpoint Security 11.9.0 for Windows.
- Kaspersky Next Expert View now supports the Japanese localization of Kaspersky Embedded Systems Security.

Update March 09, 2022

This update of Kaspersky Next Expert View includes the following new features and improvements:

- Integration with Kaspersky Endpoint Detection and Response Expert is implemented.
- Incident Response Platform (IRP) is implemented. Now you can manage security incidents via Kaspersky Next Expert View.
- Kaspersky Next Expert View now accepts license keys for Kaspersky Endpoint Detection and Response Expert. The minimum number of devices for the license is 50.

Update February 11, 2022

This update of Kaspersky Next Expert View includes the following new features and improvements:

- Licenses for Kaspersky Embedded Systems Security for Windows are now supported.
- Kaspersky Endpoint Security 11.8.0 for Windows is supported.
- You can install Kaspersky Endpoint Security 11.8.0 for Windows using a distribution package in Japanese.
- Kaspersky Endpoint Agent 3.12 is supported.

Update December 10, 2021

This update of Kaspersky Next Expert View includes the following new features and improvements:

- Work with internal users is improved:
  - You can now add new internal users on the portal.
  - The application now prevents you from decreasing your own rights.

Update October 18, 2021

This update of Kaspersky Next Expert View includes the following new features and improvements:

- Kaspersky Next Expert View now supports Kaspersky Endpoint Detection and Response Optimum 2.0.
- You can now manage mobile devices running Android by using Kaspersky Next Expert View.
- Kaspersky Marketplace is available as a new menu section: you can now search for a Kaspersky application by using Kaspersky Next Expert View.
- A new menu section, Kaspersky announcements, is available. Kaspersky announcements keep you informed by providing information related to the Kaspersky applications installed on the managed devices. Kaspersky Next Expert View periodically updates the information in the section.
- You can now manage secondary Administration Servers running under Linux operating systems via Kaspersky Next Expert View.

Update September 07, 2021

This update of Kaspersky Next Expert View includes the following new features and improvements:

- You can now use Active Directory Federation Services (AD FS) to log in to Kaspersky Next Expert View by using your Active Directory account, without creating a new user account.
- Kaspersky Next Expert View now works with the following cloud environments: Amazon Web Services, Microsoft Azure, and Google Cloud. To protect virtual machines (or instances) in a cloud environment, you need one of the Kaspersky Hybrid Cloud Security licenses. The Cloud Environment Configuration Wizard is available.
- The maximum number of devices per one workspace is now 25,000.
- Integration with SIEM systems now is available in Kaspersky Next Expert View. You can export events to SIEM systems by using the Syslog protocol.
- You can now create virtual Administration Servers. Each virtual Administration Server can have its own structure of administration groups, policies, tasks, reports, and events. You can use virtual Administration Servers for the management of client organizations with complicated workflows within your workspace. However, you cannot migrate virtual Administration Servers from Kaspersky Security Center running on-premises to Kaspersky Next Expert View.
- You can now adjust the width of columns in tables, and sort and search for data.
- We have improved the stability and availability of Kaspersky Business Hub and Kaspersky Next Expert View.

Update October 27, 2020

This update of Kaspersky Next Expert View includes the following new features and improvements:

- Kaspersky Next Expert View now supports Kaspersky Endpoint Security 11.6.0 for Windows, Kaspersky Endpoint Security 11.1 for Mac Patch A, and Kaspersky Endpoint Agent 3.10 (as part of Kaspersky Endpoint Detection and Response Optimum).
- You can now use the following licenses:
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Endpoint Security for Business Advanced
  - Kaspersky Total Security for Business
- The following features are implemented:
  - Vulnerability and patch management
  - Encryption management
  - Application Control

- Adaptive Anomaly control
- RDP sessions, including Windows Desktop Sharing

- The navigation menu is now vertical, which resembles the Microsoft Management Console-based interface of Kaspersky Security Center.
- Technical training videos are now available; they will help you to learn how the application works.

Update June 30, 2020

This update of Kaspersky Next Expert View includes the following new features and improvements:

- Kaspersky Next Expert View now supports Kaspersky Security 11 for Windows Server (starting from September, 2020).
- Kaspersky Next Expert View now supports Kaspersky Endpoint Agent 3.9 and Kaspersky Endpoint Security 11.4.0 for Windows.
- The Quick Start Wizard has been improved: some steps have been removed, the sequence of steps has been slightly changed, and some texts have been edited for usability.
- Kaspersky Next Expert View is now available in the Italian language.
- You can now revoke the End User License Agreement (EULA) for any managed Kaspersky application via the interface of Kaspersky Next Expert View. You must uninstall the selected application before revoking its EULA.
- You can now delete workspaces. If you mark a workspace for deletion, it is by default deleted automatically in seven days. However, you can force the deletion of the workspace, so that it is deleted immediately.
- Two-step verification for signing in to the console is implemented.

Fixed issues

The table below lists all issues found in previous Kaspersky Next Expert View updates, and which are fixed in the current version.

List of issues fixed in Kaspersky Next Expert View

Kaspersky Next Expert View update the issue first appeared in	Issue ID	Issue description
Update February, 2026	9526104	Fixed an issue where the tooltip text blended with the background when you selected mobile certificates.
Update June, 2026	9577592	Fixed an issue where large Kaspersky Endpoint Security policies might fail to load the **Application settings** section correctly, causing it to appear empty.
Update June, 2026	10065748	Fixed an issue where detailed information about a rule When viewing the **Report on Web Control** report in Web Console was not displayed if its name contained square brackets.
Update June, 2026	10112458	Fixed an issue where, on the **Trial mode limits**, the **Limits on application features** was missing information regarding installation packages limits.
Update June, 2026	10117987	Fixed an issue where the **Administration Server** section in the main menu was displayed in English across all non-English localizations.
Update June, 2026	10128693	Fixed an issue that caused the "**An error occurred**" message when saving a policy after making changes.
Update June, 2026	10128748	Fixed an issue that caused the application list to display incorrect Unified Protection and Management Plug-in applications when creating the **Start or stop application** task.
Update June, 2026	10183311	Fixed an issue where the **Find vulnerabilities and required updates** task might complete with the **Completed with warning** status.
Update June, 2026	10189276	Fixed an issue where a set limit on the number of security groups might not be observed correctly.
Update June, 2026	10189594	Fixed an issue where the **Dashboard** section, together with the administration group hierarchy, was incorrectly displayed if you navigated to the **Tasks** section from the **Dashboard** section by manually modifying the URL in the browser address bar.
Update February, 2026	9501104	Fixed an issue where tutorials in the corresponding section might fail to start on the first attempt.
Update June, 2026	9968154	Fixed an issue where notifications might be displayed in the incorrect language after the Web Console interface language was changed.
Update June, 2026	10076008	Fixed an issue where the light mode may momentarily appear instead of the dark mode while navigating between sections during page loading.
Update June, 2026	10076016	Fixed an issue where a user whose relevant permissions had been just revoked could still download a report on existing licenses containing up-to-date data.
Update June, 2026	10112524	Fixed an issue where an unnecessary `ui_locales` parameter was displayed in the URL after switching localizations.
Update June, 2026	10126364	Fixed an issue where you could switch from a commercial license to a trial license.
Update June, 2026	10128638	Fixed an issue where a user might not be displayed correctly in the **Users & roles** → **Roles** section after assigning custom permissions to a user in the administration group's properties .
Update June, 2026	10146377	Fixed an issue where, if the MDR section was set as the home page, it remained the home page even after the **Show MDR features** option was disabled in **Settings** → **Interface options** section.
Update June, 2026	10157485	Fixed an issue where data from the **Software vulnerabilities** section was exported incorrectly to CSV and TXT formats.

Kaspersky Next Expert View

Kaspersky Next Expert View is an application aimed at corporate network administrators and employees responsible for protection of devices in a wide range of organizations. It provides extensive options for the protection of your users' devices and is recommended for large businesses. Kaspersky Next Expert View is hosted and maintained by Kaspersky. You do not have to install Kaspersky Next Expert View on your computer or server.

Kaspersky Next Expert View enables you to do the following:

- Install Kaspersky applications on devices on your network and manage the installed applications.
- Create a hierarchy of administration groups to manage a selection of client devices as a whole.
- Create virtual Administration Servers and arrange them in a hierarchy.
- Protect your network devices, including workstations and servers:
  - Manage an antimalware protection system built on Kaspersky applications.
  - Use the detection and response (EDR and MDR) capabilities (a license for Kaspersky Endpoint Detection and Response and/or for Kaspersky Managed Detection and Response is required), including:
    - Analyzing and investigating incidents
    - Incident visualization through creating a threat development chain graph
    - Accepting or rejecting responses manually or setting up the auto-accept of all responses
- Use Kaspersky Next Expert View as a multi-tenant application.
- Remotely manage Kaspersky applications installed on client devices.
- Perform centralized deployment of license keys for Kaspersky applications to client devices.
- Create and manage security policies for devices on your network.
- Create and manage user accounts.
- Create and manage user roles (RBAC).
- Create and manage tasks for applications installed on your network devices.
- View reports on the security system status for every client organization individually.

Before using Kaspersky Next Expert View, you must create an account and a workspace.

You manage Kaspersky Next Expert View by using Web Console that ensures interaction between your device and Administration Server over a browser. Administration Server is an application designed for managing Kaspersky applications installed on your network devices. When you connect to Kaspersky Next Expert View by using your browser, the browser establishes a connection with Kaspersky Next Expert View Server.

The Administration Server and connected database management system (DBMS) are deployed in a cloud environment and provided to you as a service. Maintenance of both the Administration Server and the DBMS is carried out as part of the service offering. All software components of Kaspersky Next Expert View are kept up-to-date. The Administration Server and created objects (such as policies and tasks) are backed up regularly to keep them safe.

Kaspersky Next Expert View is a multi-language application. You can change the interface language at any time, without reopening the application.

> 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.

Hardware and software requirements for Kaspersky Next Expert View

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 Console

For a client, the use of Kaspersky Next Expert View requires only a browser.

> You can only use a single browser window or tab to work with Kaspersky Next Expert View.

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 Next Expert View.

Browsers:

- Google Chrome 145.0.7632.26 or later
- Microsoft Edge 145.0.3800.65 or later
- Safari 18.6 on macOS
- Mozilla Firefox Extended Support Release 140.7.1.2 or later

Network Agent

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.

Minimum hardware requirements for Vulnerability and patch management:

- CPU with operating frequency of 1.4 GHz or higher. A 64-bit OS is required.
- RAM: 8 GB
- Free disk space: 1 GB.

> The Arm architecture is not supported.

Operating systems. Microsoft Windows workstations	Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32-bit Microsoft Windows Embedded 7 Standard with Service Pack 1 32-bit/64-bit Microsoft Windows Embedded 8.1 Industry Pro 32-bit/64-bit Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit Microsoft Windows 10 Enterprise 2016 LTSB 32-bit/64-bit Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-bit/64-bit Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-bit/64-bit Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit Microsoft Windows 10 IoT Enterprise version 1703, 1709, 1803, 1809 32-bit/64-bit Microsoft Windows 10 20H2, 21H2 IoT Enterprise 32-bit/64-bit Microsoft Windows 10 IoT Enterprise 32-bit/64-bit Microsoft Windows 10 IoT Enterprise version 1909 32-bit/64-bit Microsoft Windows 10 IoT Enterprise LTSC 2021 32-bit/64-bit Microsoft Windows 10 IoT Enterprise version 1607 32-bit/64-bit Microsoft Windows 10 TH1 (July 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 TH2 (November 2015) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 RS1 (August 2016) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 RS2 (April 2017) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 RS4 (April 2018 Update, 17134) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 RS5 (October 2018) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 RS6 (May 2019) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 20H1 (May 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 20H2 (October 2020 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 21H1 (May 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 21H2 (October 2021 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 10 22H2 (October 2023 Update) Home/Pro/Pro for Workstations/Enterprise/Education 32-bit/64-bit Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-bit Microsoft Windows 8.1 Pro/Enterprise 32-bit/64-bit Microsoft Windows 8 Pro/Enterprise 32-bit/64-bit Microsoft Windows 7 Home/Pro/Enterprise/Ultimate with Service Pack 1 and later 32-bit/64-bit 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) 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 Microsoft Windows Server 2008 Standard/Enterprise/Datacenter/Foundation with Service Pack 2 32-bit/64-bit Microsoft Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation with Service Pack 1 and later 64-bit Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64-bit Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64-bit Microsoft Windows Server 2016 Server Core/Datacenter/Essentials/Standard (Installation Option) (LTSB) 64-bit Microsoft Windows Server 2019 Standard/Datacenter/Core 64-bit Microsoft Windows Server 2019 RS5 Essentials/Standard 64-bit Microsoft Windows Server 2022 Standard/Datacenter/Core 64-bit Microsoft Windows Server 2022 21H2 Standard/Datacenter 64-bit Microsoft Windows Server 2025 Standard/Datacenter/Core 64-bit Microsoft Windows Small Business Server 2011 Standard/Essentials/Premium Add-on 64-bit
Operating systems. Linux	Debian GNU/Linux 13 (Trixie) 64-bit Debian GNU/Linux 12 (Bookworm) 32-bit/64-bit Debian GNU/Linux 11.x (Bullseye) 32-bit/64-bit Ubuntu Server 24.04 LTS 64-bit Ubuntu Server 22.04 LTS 64-bit Ubuntu Server 20.04 LTS (Focal Fossa) 64-bit CentOS 7.x 64-bit CentOS Stream 10 64-bit CentOS Stream 9 64-bit CentOS Stream 8 64-bit Red Hat Enterprise Linux Server 10.x 64-bit Red Hat Enterprise Linux Server 9.x 64-bit Red Hat Enterprise Linux Server 8.x 64-bit Red Hat Enterprise Linux Server 7.x 64-bit openSUSE Leap 15 64-bit SUSE Linux Enterprise Server 15 (all Service Packs) 64-bit SUSE Linux Enterprise Server 12 (all Service Packs) 64-bit Oracle Linux 7 64-bit Oracle Linux 8 64-bit Oracle Linux 9 64-bit Linux Mint 21.x 64-bit Linux Mint 22.x 64-bit Alma Linux 8.x 64-bit Alma Linux 9.x 64-bit Rocky Linux 8.x 64-bit Rocky Linux 9.x 64-bit Amazon Linux 2 64-bit Kylin 10 64-bit
Operating systems. macOS	For the list of supported operating systems, refer to the Kaspersky Endpoint Security for Mac Help.

For Network Agent, the Apple Silicon (M1) architecture is also supported, as well as Intel.

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

Before installing Network Agent on the devices running Windows 7, Windows Server 2008 or Windows Server 2008 R2, 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 (KB3063858), Security Update for Windows Server 2008 x64 Edition (KB3063858), Security Update for Windows Server 2008 R2 x64 Edition (KB3063858).

Compatible Kaspersky applications and solutions

Licenses for different products grant different sets of Kaspersky applications and solutions.

You can deploy and manage the following Kaspersky applications and solutions via Kaspersky Next Expert View:

- Kaspersky Endpoint Security 14.1 for Windows (only Lite encryption (AES56) is supported)
- Kaspersky Endpoint Security 12.5 for Linux
- Kaspersky Endpoint Security 12.2 for Mac
- Kaspersky Embedded Systems Security 4.0 for Windows
- Kaspersky Embedded Systems Security 4.0 for Linux
- Kaspersky Endpoint Agent 4.0
- Kaspersky Endpoint Security for Android
- Kaspersky Security for iOS

You can integrate the following solutions to view and process security incidents:

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

If you install a new application version on a managed device, but use an outdated policy for the new application version rather than update the policy, the application still provides data to Kaspersky Next Expert View, but Kaspersky Next Expert View cannot process this data as described in the Processed data of managed applications section of the documentation. For Kaspersky Next Expert View to process this data, you must create a new policy for the new version of the application.

Localization of Kaspersky Next Expert View

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

Comparison of Kaspersky Security Center and Kaspersky Next Expert View

You can use Kaspersky Security Center in the following ways:

- As a cloud solution

  Kaspersky Security Center is installed for you in 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.

- As an on-premises solution (Windows-based or Linux-based)

  You install Kaspersky Security Center on a local device and manage the network security system through the Microsoft Management Console-based Administration Console or Kaspersky Security Center Web Console.

  In addition to the Windows-based application, Kaspersky Security Center Linux is also available. Kaspersky Security Center Linux is designed to deploy and manage protection of Linux devices by using Linux-based Administration Server to meet the requirements of pure Linux environments. The Windows-based Kaspersky Security Center and Kaspersky Security Center Linux have different sets of features.

The table below lets you compare the main features of Kaspersky Security Center and Kaspersky Next Expert View.

Feature comparison of Kaspersky Security Center running on-premises and as a cloud solution

Feature or property	Kaspersky Security Center running on-premises	Kaspersky Next Expert View
Administration Server location	On-premises	Cloud environment
Database management system (DBMS) location	On-premises	Cloud environment
Web-based administration console	✓	✓
Maintenance of Administration Server and DBMS	Managed by customer	Managed by Kaspersky
Hierarchy of Administration Servers	✓	✓ (Administration Server of Kaspersky Next Expert View can only act as a primary Administration Server in the hierarchy and can only be used for policies and tasks monitoring)
Administration group hierarchy	✓	✓
Migration of the managed devices and related objects from Kaspersky Security Center on-premises to Kaspersky Next Expert View	✓	✓
Network polling	✓	✓ (by distribution points only)
Maximum number of managed devices	100,000	25,000
Protection of Windows, Linux, and macOS managed devices	✓	✓
Protection of mobile devices	✓	✓ (only Kaspersky Endpoint Security for Android and Kaspersky Security for iOS are supported)
Protection of public cloud infrastructure	✓	✓
Device-centric security management	✓	✓
Application policies	✓	✓
Tasks for Kaspersky applications	✓	✓
Kaspersky Security Network	✓	✓
KSN proxy server	✓	✓ (on distribution points only)
Kaspersky Private Security Network	✓	—
Centralized deployment of license keys for Kaspersky applications	✓	✓
Switching managed devices to another Administration Server	✓	— (you must reinstall Network Agents on managed devices to switch them to another Administration Server)
Support for virtual Administration Servers	✓	✓
Installing third-party software updates and fixing third-party software vulnerabilities	✓	✓ (to fix third-party software vulnerabilities, only recommended fixes can be installed)
Notifications about events occurred on managed devices	✓	✓
Creating and managing user accounts	✓	✓
Maximum number of events in the database	400,000 (can be increased up to 45,000,000)	400,000
Integration with SIEM systems	✓	✓ (by using the Syslog format and TLS over TCP protocol only)
Using Administration Server as WSUS server	✓	—
Monitoring the statuses of policies and tasks	✓	✓

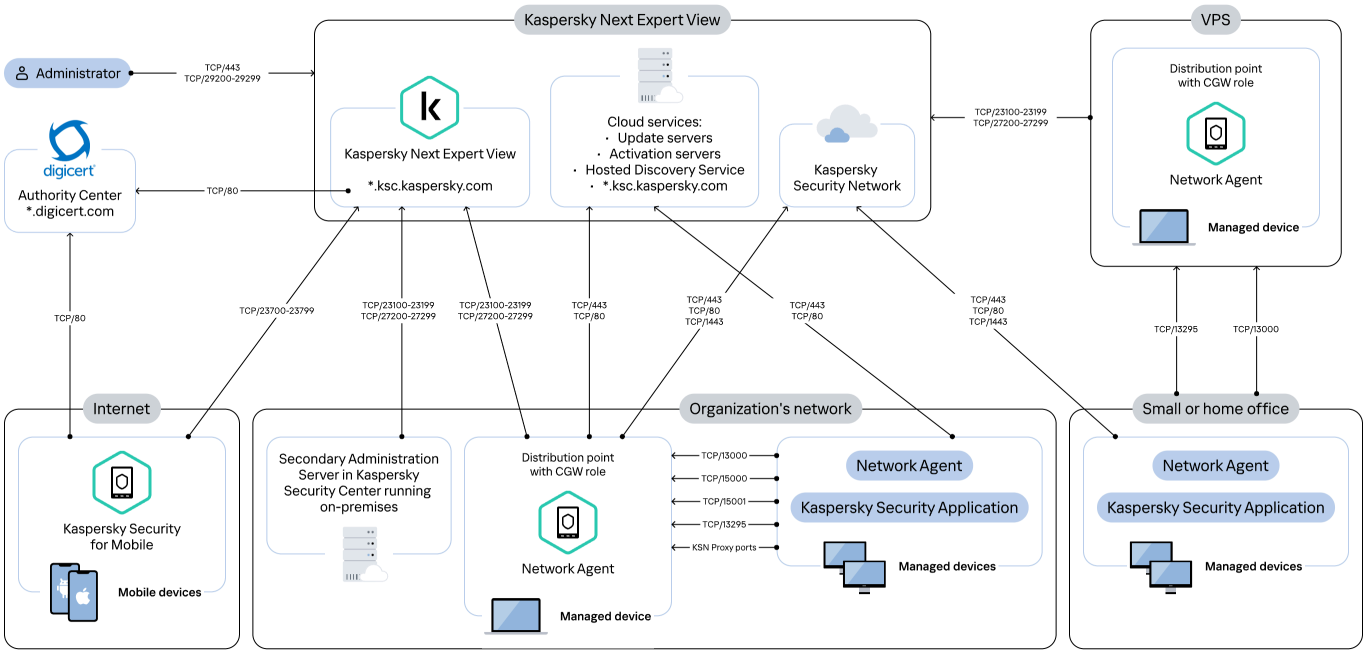
Feature or property	Kaspersky Security Center running on-premises	Kaspersky Next Expert View
Support of clusters and server arrays in administration groups	✓	✓
Remote installation of operating systems	✓	—
SNMP support	✓	—
Maximum number of virtual Servers	500	200
Cloning the hard drive of a device	✓	—
OpenAPI support	✓	—

Architecture and basic concepts

This section explains the application architecture and basic concepts related to Kaspersky Next Expert View.

Architecture

This section provides a description of the components of Kaspersky Next Expert View and their interaction.



Kaspersky Next Expert View architecture

Kaspersky Next Expert View managed via the cloud-based console includes two main components: Kaspersky Next Expert View infrastructure and customer's infrastructure.

Kaspersky Next Expert View infrastructure consists of the following:

- **Cloud-based Administration Console**. Provides a web interface for creating and maintaining the protection system of a client organization's network that is managed by Kaspersky Next Expert View.
- **Cloud services**. Includes update servers and activation servers.
- **Kaspersky Security Network (KSN)**. Servers that contain a Kaspersky database with continuously 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.

Customer's infrastructure may consist of the following:

- **Distribution point**. 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.

- **Managed devices**. Computers of customer's network protected through Kaspersky Next Expert View. Network Agent and a Kaspersky security application must be installed on each managed device.

- **Secondary Administration Server running on-premises** (optional). You can use an on-premises Administration Server to create a hierarchy of Administration Servers.

Ports used by Kaspersky Next Expert View

To use Kaspersky Next Expert View, which is part of the Kaspersky infrastructure, you must open the following ports on the client devices to allow the internet connection (see table below):

Ports that must be open on client devices to allow the internet connection

Port (or port range)	Protocol	Purpose of the port (or port range)
23100-23199	TCP/TLS	Receiving connections from Network Agents and secondary Administration Servers on Kaspersky Next Expert View Administration Server at *.ksc.kaspersky.com. The Kaspersky infrastructure can use any port within this range and any web address within this mask. The port and the web address can change from time to time.
23700-23799 (only if you manage mobile devices)	TCP/TLS	Receiving connections from mobile devices. Connection to the Kaspersky Next Expert View Administration Server at *.ksc.kaspersky.com. The Kaspersky infrastructure can use any port within this range and any web address within this mask. The port and the web address can change from time to time.
27200-27299	TCP/TLS	Receiving connections for application activation from managed devices (except for mobile devices). Connection to the Kaspersky Next Expert View Administration Server at *.ksc.kaspersky.com. The Kaspersky infrastructure can use any port within this range and any web address within this mask. The port and the web address can change from time to time.
29200-29299	TCP/TLS	Tunneling connections to managed devices by using the klsctunnel utility through Kaspersky Next Expert View Administration Server at *.ksc.kaspersky.com. The Kaspersky infrastructure can use any port within this range and any web address within this mask. The port and the web address can change from time to time.
443	HTTPS	Connection to Kaspersky Next Expert View discovery service at *.ksc.kaspersky.com. The Kaspersky infrastructure can use any web address within this mask.
1443	TCP	Connection to Kaspersky Security Network
80	TCP	Connection is used to check validity of the Kaspersky Security Center certificates at *.digicert.com. The Kaspersky infrastructure can use any web address within this mask.

The table below lists the ports that must be open on client devices where Network Agent is installed.

Ports that must be open on client devices

Port number	Protocol	Port purpose	Scope
15000	UDP	Receiving data from connection gateways (if in use)	Managing client devices
15000	UDP broadcast	Getting data about other Network Agents within the same broadcasting domain	Delivering updates and installation packages
15001	UDP	Receiving multicast requests from a distribution point (if in use)	Receiving updates and installation packages from a distribution point

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 Next Expert View 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 lists the additional ports that must be open on client devices where Network Agent is installed as a distribution point.

Ports used by Network Agent functioning as distribution point

Port number	Protocol	Port purpose	Scope
13000	TCP/TLS	Receiving connections from Network Agents	Managing client devices and delivering updates and installation packages
13111 (only if KSN proxy service is run on the device)	TCP	Receiving requests from managed devices to KSN proxy server	KSN proxy server
13295 (only if you use the distribution point as a push server)	TCP/TLS	Sending push notifications to managed devices	Distribution point used as a push server
15111 (only if KSN proxy service is run on the device)	UDP	Receiving requests from managed devices to KSN proxy server	KSN proxy server
17111 (only if KSN proxy service is run on the device)	HTTPS	Receiving requests from managed devices to KSN proxy server	KSN proxy server

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	Only for Linux-based client devices. Remote installation of Kaspersky applications through a Linux distribution point.

If you have one or more Administration Servers on your network and use them as secondary Administration Servers when the primary Administration Server is located in the Kaspersky infrastructure, please refer to the list of ports that are used by Kaspersky Security Center and Kaspersky Security Center Linux running on-premises. Use those ports for interaction between your secondary Administration Server (or secondary Administration Servers) and client devices.

Basic concepts

This section explains basic concepts related to Kaspersky Next Expert View.

Network Agent

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

Network Agent 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

A device that has Network Agent installed is called a *managed device* or *device*. You can install Network Agent on a Windows, Linux, or Mac device.

The name of the process that Network Agent starts is *klnagent.exe*.

Network Agent synchronizes the managed device with the Administration Server. Kaspersky Next Expert View automatically synchronizes the Administration Server with the managed devices several times per hour. The Administration Server sets the synchronization interval (also referred to as the *heartbeat*) depending on the number of managed devices.

Administration groups

An *administration group* (hereinafter also referred to as a *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 Next Expert View.

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 computer from the Accountants administration group to the Developers administration group. Thereafter, the device will automatically receive the application settings required for developers.

Hierarchy of Administration Servers

Administration Servers can be arranged in a "primary/secondary" hierarchy. Each Administration Server can have several secondary Administration Servers on different nesting levels of the hierarchy. The nesting level for secondary Administration Servers is unrestricted. The administration groups of the primary Administration Server will then include the client devices of all secondary Administration Servers.

Kaspersky Next Expert View Administration Server can only act as a primary Administration Server and can have as secondary Servers only Administration Servers running on-premises.

When migrating from the Administration Server that runs on-premises to the Kaspersky Next Expert View Administration Server, you can arrange the Administration Servers in a hierarchy. Then, to mitigate the migration, you can shift only part of your managed devices to the management of the Kaspersky Next Expert View Administration Server. The rest of the managed devices remain under the management of the on-premises Administration Server. This enables you to test management features of Kaspersky Next Expert View on a limited number of managed devices. At the same time, you can configure policies, tasks, reports and other objects to test management and monitoring of your entire network. This lets you switch back to the objects configured on the on-premises Administration Server if necessary.

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 Administration Servers based on network attributes.

Virtual Administration Server

Virtual Administration Server (also referred to as *virtual Server*) is a component of Kaspersky Next Expert View intended for managing anti-virus protection of the network of a client organization. Each virtual Administration Server can have its own structure of administration groups and its own means of management and monitoring, such as policies, tasks, reports, and events. The functional scope of virtual Administration Servers can be used by organizations with complicated workflows.

Virtual Administration Server has the following restrictions:

- Virtual Administration Servers are supported only in the commercial mode of Kaspersky Next Expert View.
- Virtual Server does not support creation of secondary Administration Servers (including virtual Servers).
- You cannot migrate virtual Administration Servers from Kaspersky Security Center to Kaspersky Next Expert View.
- By default, the administrator that manages the primary Administration Server also manages all of the virtual Administration Servers.

- Users created on a virtual Server cannot be assigned a role on the Administration Server.
- In the virtual Administration Server properties window, the number of sections is limited.

Distribution point

A *distribution point* is a device with Network Agent installed that is used for update distribution, remote installation of applications, and retrieval of information about networked devices. Distribution points can also act as Connection Gateways to reduce the number of outgoing external connections and the number of simultaneous connections to the Administration Server.

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 to client devices within the group (including distribution through multicasting using UDP). Updates can be received from Kaspersky update servers through an update task created for the distribution point.

  Distribution point devices running macOS cannot download updates from Kaspersky update servers.

  If one or more devices running 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.

- Distribute policies and group tasks through multicasting using UDP.
- Act as a gateway for connections with the Administration Server because in a cloud infrastructure, it is often impossible to establish a direct connection between network devices and the Administration Server. A connection gateway optimizes network connections and reduces the load on the Administration Server.
- Poll the network to detect new devices and update information about existing ones.
- Perform remote installation of third-party software and Kaspersky applications through Microsoft Windows tools, 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 the Kaspersky Security Network.

  This feature is not supported by distribution point devices running macOS.

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

If you have more than 10,000 devices, multiple virtual Servers and policies, we strongly recommend using distribution points for the correct function of your infrastructure. When assigning a device to act as a distribution point, refer to the Calculating the number and configuration of distribution points article.

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 reducing traffic.

The scope of a distribution point is one or more administration groups to which it has been assigned by the administrator, as well as subgroups of all levels of embedding. However, the device acting as the distribution point may not be included in the administration group to which it has been assigned. 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.

One or more network location can also be the scope of distribution points. The network locations are used for manual creation of a set of devices to which the distribution point will distribute updates. Determining a network location is available for devices running a Windows or Linux operating system.

Kaspersky Next Expert View 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.

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 Next Expert View 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.

Management web plug-in

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

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 Next Expert View 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 Next Expert View provides a single policy for each Kaspersky application in an administration group. A policy has one of the following statuses (see the table below):

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.
- You can activate an inactive policy when a specific event occurs. For example, you can enforce stricter anti-virus protection settings during virus outbreaks.
- 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 Next Expert View 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.

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.

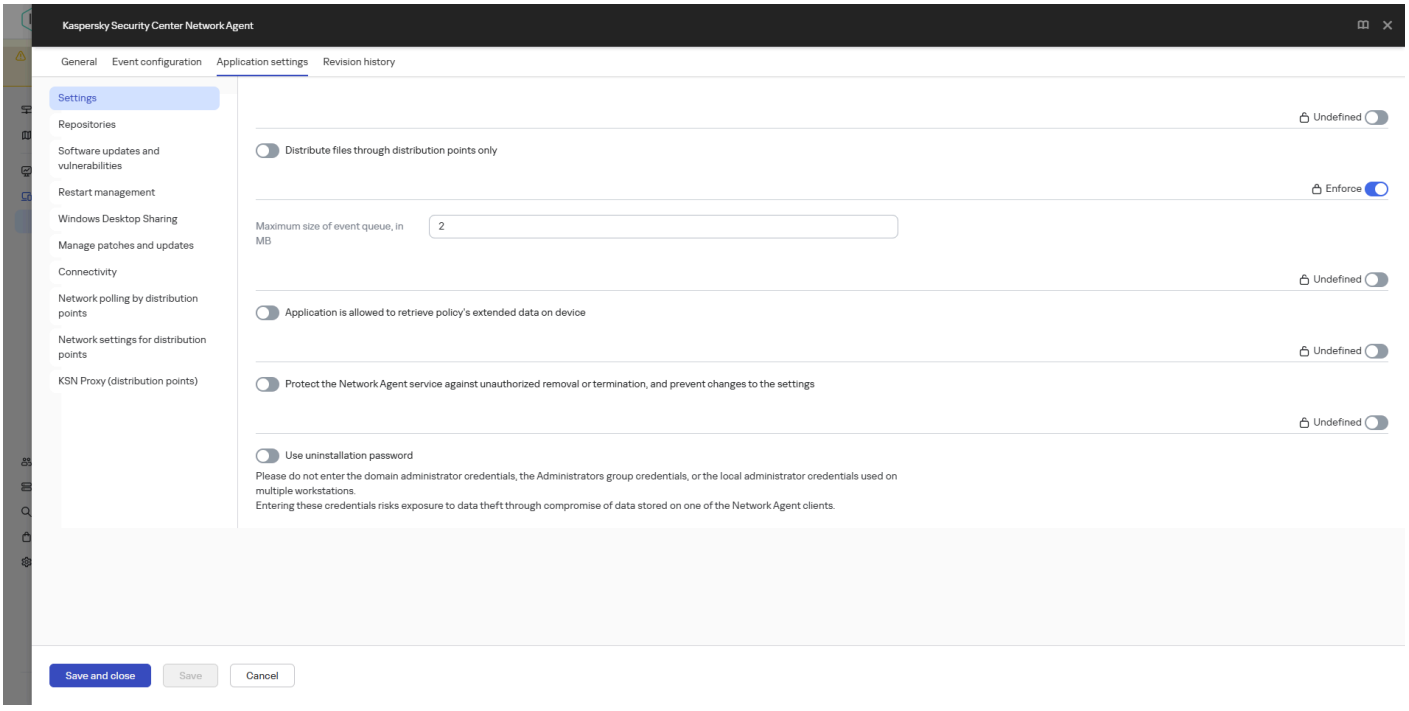
The value of a setting that the application uses on a client device is defined by the lock position (🔒) for that setting in the policy:

- 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.



Application settings of the policy

Application licensing

This section provides information related to the application licensing.

Licensing of Kaspersky Next Expert View

Following this scenario, you can start using Kaspersky Next Expert View and managed security applications under a license.

Kaspersky Next Expert View enables you to perform centralized distribution of license keys for Kaspersky applications on client devices, monitor their use, and renew licenses.

If you are already using Kaspersky Next Expert View, you can visit Kaspersky Marketplace to view the entire range of Kaspersky business solutions, select the ones you need, and proceed to the purchase at the Kaspersky website.

Checking out the features of Kaspersky Next Expert View in the trial mode before purchasing a license

You can first to try Kaspersky Next Expert View for free. To do this, create a trial workspace which will terminate in 30 days. If you want a commercial workspace that you can use as long as you want, you will have to purchase a license.

Stages

The scenario proceeds in stages:

1. **Getting an activation code for licensing Kaspersky Next Expert View in the commercial mode. Purchasing a license (or licenses)**

   Different licenses grant the usage of different Kaspersky applications and services, so you might want to purchase more than one license.

   Find out what licenses that you can purchase and the minimum number of devices for each license.

   Kaspersky Next Expert View comes as part of several Kaspersky solutions. Choose what solution you want to use and purchase a license for it. You will need to contact Kaspersky or one of Kaspersky partners with a special request if you want to purchase a license that covers 10,000 or more devices.

   Use the table to check which Vulnerability and patch management features are available under which license.

   If you want to use Kaspersky Next Expert View in a cloud environment such as Microsoft Azure, read about the licensing options for cloud environments.

   If you are a Manage Service Provider (MSP), read about licensing of Kaspersky Next Expert View for MSPs.

2. **Activation of Kaspersky Next Expert View when creating the workspace**

   You specify your license key to activate Kaspersky Next Expert View when creating a workspace.

   If you have multiple license keys, specify any of your license keys. Later you will need to add other license keys to Kaspersky Next Expert View to activate managed Kaspersky applications.

3 Adding license keys for managed applications to the Administration Server repository

Before deployment of the license keys, you must add these license keys to the Administration Server repository.

The license key that you specified when creating the workspace is automatically added to the Administration Server repository.

If you have more than one license keys, add your license keys one by one to the Kaspersky Next Expert View Administration Server repository.

4 Deploying license keys for managed applications

Choose a method of deployment of the license key (or license keys) to all the devices you want to protect:

- Automatic deployment

  > If you use different managed applications and you have to deploy a specific activation code for applications, choose another way of deploying that activation code.

  Kaspersky Security Center enables you to automatically deploy available license keys for managed applications. For example, three license keys are stored in the Administration Server repository. You have enabled the **Automatically distribute license key to managed devices** option for all three license keys. A Kaspersky security application—for example, Kaspersky Endpoint Security for Windows—is installed on the organization's devices. A new managed application on a device is discovered for which a license key must be deployed. For instance, two of the license keys from the repository can be deployed for the managed application on the device: license key named *Key_1* and license key named *Key_2*. One of these license keys is deployed for the managed application. In this case, it cannot be predicted which of the two license keys will be deployed because automatic deployment of license keys does not provide for any administrator activity.

  When a license key is deployed, the number of installations is recounted for that license key. You must make sure that the number of applications for which the license key was deployed does not exceed the license limit. If the number of installations exceeds the license limit, all devices that were not covered by the license will be assigned *Critical* status.

  How-to instructions:

  - Adding a license key to the Administration Server repository
  - Automatic distribution of a license key

- 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.

  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.

5 Checking on which devices the managed Kaspersky applications are activated

To make sure that the license keys are deployed correctly, view the list of the license keys that are used for an application.

6. **Configuring events related to the license expiration**

   Configure events so that you will be notified when your license keys are used up or about to expire:

   - Administration Server critical events
   - Administration Server functional failure events
   - Administration Server warning events
   - Administration Server informational events

About the trial mode of Kaspersky Next Expert View

The *trial mode* is a special mode of Kaspersky Next Expert View intended to acquaint the user with the features of Kaspersky Next Expert View. When you start using Kaspersky Next Expert View, you can either request a trial workspace or enter an activation code for a commercial license. If a trial workspace is requested, a 30-day trial license is automatically embedded into the workspace. The set of features available in trial mode is equivalent to that provided under the Kaspersky Next EDR Optimum license.

If the application is activated with a commercial license before the trial expiration date, the workspace configuration and all previously added devices are preserved. Otherwise, the workspace and all its data will automatically be deleted upon expiration of the trial period.

The following restrictions are imposed on the use of the Expert View features in trial mode:

- You cannot create a hierarchy of Administration Servers. No virtual Administration Servers can be created.
- You cannot create custom installation packages.
- You cannot create custom roles for users.
- The Virus outbreak feature is not available. Virus outbreak events are not stored, and no notifications are sent.
- The **Deleted objects** repository is not available.
- You cannot enable the addition of batched events (those published in large quantities) to the database.
- Migration of Administration Servers from on-premises mode to Web Console mode is not supported.
- KSN statistical information from the Administration Server components, such as Administration Server or Network Agent, is not sent to Kaspersky.
- Integration with Active Directory Federation Services (AD FS) is not supported.
- Integration with Microsoft Entra ID is not supported.

Some limits are also imposed on creation of some objects of the application (see the table below). If any of these limits are exceeded when an attempt is made to create such an object, the object creation will be blocked, and an error message about the limit will be displayed.

Limitations on creating Expert View objects in trial mode

Type of limitation	Value
Policies	30
Tasks	30
License keys	5
Packages	8
Device selections (preset instances not included)	5
Event selections (preset instances not included)	5
Device moving rules	3
Report templates of the same type	10
Internal security groups	20
Managed devices	500

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 Next Expert View 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.

Licenses and the minimum number of devices for each license

If you want to use Kaspersky Next Expert View in commercial mode, you must purchase a license before creating your first workspace. The table below shows the licenses that you can purchase and the minimum number of devices for each license (even if you want to protect fewer devices):

Licenses that grant the usage of Kaspersky Next Expert View

License	Minimum number of devices (even if you want to protect a fewer number)
Kaspersky Endpoint Security for Business Select	For commercial licenses: 300 For commercial (subscription) licenses: 100
Kaspersky Endpoint Security for Business Advanced	For commercial licenses: 300 For commercial (subscription) licenses: 100
Kaspersky Total Security for Business	300
Kaspersky Endpoint Detection and Response Optimum	For commercial licenses: 300 For commercial (subscription) licenses: 100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Hybrid Cloud Security, Desktop	For commercial licenses: 300 For commercial (subscription) licenses: 100
Kaspersky Hybrid Cloud Security, Server	50
Kaspersky Hybrid Cloud Security, Core	20
Kaspersky Hybrid Cloud Security, CPU	20
Kaspersky Hybrid Cloud Security Enterprise, Desktop	For commercial licenses: 300 For commercial (subscription) licenses: 100

License	Minimum number of devices (even if you want to protect a fewer number)
Kaspersky Hybrid Cloud Security Enterprise, Server	50
Kaspersky Hybrid Cloud Security Enterprise, CPU	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security Compliance Edition	300
Kaspersky Symphony (currently only available in Russia)	300
Kaspersky Next EDR Foundations	100 users Each user license can apply to 1 PC/Mac device and 2 mobile devices.
Kaspersky Next EDR Optimum	100 users Each user license can apply to 1 PC/Mac device and 2 mobile devices.
Kaspersky Next Complete Security	100 users Each user license can apply to 1 PC/Mac device and 2 mobile devices.
Kaspersky Next EDR Expert	100 users Each user license can apply to 1 PC/Mac device and 2 mobile devices.
Kaspersky Next XDR Expert	100 users Each user license can apply to 1 PC/Mac device and 2 mobile devices.
Kaspersky Next MXDR Optimum	150 users
Kaspersky XDR Optimum (currently only available in Russia and CIS)	For commercial licenses: 300 users For commercial (subscription) licenses: 100 users
Kaspersky Next XDR Optimum	100 users Each user license can apply to 1 PC/Mac device and 2 mobile devices.

If you want to protect more than 10,000 devices, you have to send a request to Kaspersky Technical Support and specify information about the workspace that you want to create.

Events of the license limit exceeded

Kaspersky Next Expert View 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.

Methods of distribution of the activation codes to the managed devices

The Kaspersky applications installed on managed devices must be licensed by applying an activation code to each of the applications. You cannot use key files for licensing of managed applications; only activation codes are accepted. An activation code can be deployed in the following ways:

- Automatic deployment
- The Add license key task for a managed application
- Manual activation of a managed application

Kaspersky applications can use more than one license key at the same time. For example, Kaspersky Endpoint Security for Windows can use two license keys—one for Kaspersky Endpoint Security for Windows and one for activation of the Endpoint Detection and Response functions.

In addition, Kaspersky applications can have not only an active license key, but also a reserve license key. A Kaspersky application uses an active key at the current moment and stores a reserve key to apply after the active key expires. You can add a new active or reserve license key by any of the methods listed above. 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.

Adding an Administration Server license key

To add an Administration Server license key:

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 **License keys** section, and then click the **Select** button in one of the following sections:

   - **Current license**, if you want to add an active license key.
   - **Reserve license key**, if you want to add a reserve license key.

     > You can add a reserve license key only if an active license key has already been added.

3. In the window that opens, select a required license key from the table.

   If necessary, you can add a new license key by clicking the **Add new license key** button, and then entering the license key in the right pane that opens.

4. Click **OK**.

The window is closed, the Administration Server license key is added, and information about the license key is displayed in the **License keys** section.

If necessary, you can change the selected license key by clicking the **Change** button and specifying another license key. Also, you can remove a license key.

Adding a license key to the Administration Server repository

When adding a license key using Kaspersky Next Expert View, 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.

To add a license key to the Administration Server repository:

1. In the main menu, go to **Operations** → **Licensing** → **Licenses**.
2. Click **Add**.
3. 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 Next Expert View 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 **Asset management** → **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.

6. Select devices to which the task will be assigned.

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.

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.

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.

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 Next Expert View 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** → **Licenses**.
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, switch the toggle button to **Automatically distribute license key to managed devices**.
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 license 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.

If you specify the **Automatically distribute license key to managed devices** option for a subscription license key for activating any application on a managed device, and at the same time you have an active trial license key, then your trial license key will be automatically replaced by the subscription license key eight days before the expiration date.

Viewing information about license keys in use in the Administration Server repository

To view the list of the license keys added to the Administration Server repository,

In the main menu, go to **Operations** → **Licenses**.

The displayed list contains the activation codes added to the Administration Server repository.

To view detailed information about a license key:

1. In the main menu, go to **Operations** → **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.

Viewing information about the license keys used for a specific Kaspersky application

To learn what license keys are in use for a Kaspersky application:

1. In the main menu, go to **Asset management** → **Assets (Devices)**.

   If the device belongs to the Unassigned devices group, in the main menu, go to **Discovery & deployment** → **Unassigned devices**.

2. Click the name of the required device.

3. In the device properties window that opens, select the **Applications** section.

4. In the list of applications that opens, select the application whose license keys you want to view.

5. In the application properties window that opens, on the **General** tab, select the **License keys** section.

   The information is displayed in the workspace of this section.

Removing an Administration Server license key

To remove an Administration Server license key:

1. In the main menu, click the Administration Server name.

2. In the Administration Server properties window that opens, select the **License keys** section.

3. Click the **Remove active license key** or **Remove reserve license key** button depending on the license key that you want to remove, and then in the window that opens, confirm the operation.

This removes the license key.

If a reserve license key has been added, the reserve license key automatically becomes the active license key after the former active license key is removed.

After the active license key of Administration Server is removed, Vulnerability and patch management and Mobile Device Management become unavailable. You can add a removed license key again or add a new one.

Deleting a license key from the repository

You can remove a license key from the Administration Server repository. Note that Kaspersky Next Expert View automatically deletes your workspace after 90 days in the following cases:

- You remove the last license key (active, reserve, or not in use) added manually in the repository.
- The last license key expires.

If your workspace is deleted, you cannot manage the protection of your network by means of Kaspersky Next Expert View. You also permanently lose your data from Kaspersky Next Expert View. If necessary, you can delete your workspace manually. Otherwise, we recommend that you keep at least one license key in the Administration Server repository.

If you remove a license key and you added a reserve license key earlier, the reserve license key automatically becomes the active license key after the former active key is removed or expired.

When you remove the active license key that is deployed to a managed device, the application will continue working on the managed device.

To remove a license key from the Administration Server repository:

1. Check that Administration Server does not use a license key that you want to remove. If the Administration Server does, you cannot remove the key. To run the test:

   a. Open the Administration Server properties window:

      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.

   b. In he Administration Server properties window that opens, on the **General** tab, select the **License keys** section.

   c. If the required license key 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 license key is not displayed, the Administration Server does not use it.

2. In the main menu, go to **Operations** → **Licenses**.

3. Select the required license key, and then click the **Delete** button.

4. In the window that appears, select the **I understand the risk and want to remove the license key** check box. This means that if you remove the last license key, you are aware of the subsequent deletion of the workspace and loss of control over the managed devices. Next, click the **Remove** button.

As a result, the selected license key is removed from the repository.

You can add a removed license key again or add a new one. If you removed the last license key, you can also add a license key as long as your workspace is not deleted. Kaspersky Next Expert View notifies administrators of the workspace 30 days, 7 days, and 1 day prior to deletion.

Viewing the list of devices where a Kaspersky application is not activated

You can view the list of all the devices on which a Kaspersky application is installed but not activated (for example, a license is missing or has expired).

To view the devices where a Kaspersky application is not activated:

1. In the main menu, go to **Asset management** → **Tasks**.

   The list of tasks is displayed.

2. Click the name of the Update task related to the Kaspersky application in question.

   The task properties window is displayed with several named tabs.

3. In the task properties window, select the **Results** section.

   In the **Device or secondary Server** column are displayed the devices on which the task was successful.

4. Sort the **Device or secondary Server** column.

   In the **Device or secondary Server** column are displayed the devices on which the task was successful. The devices where the task failed because of a missing license are devices where the application is not activated.

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 and its installation packages before revoking its EULA. The installation packages must be deleted from the Administration Server and its virtual Administration Servers.

The EULAs that were accepted on a virtual Administration Server can be revoked on the virtual Administration Server or on the primary Administration Server. The EULAs that were accepted on a primary Administration Server can be revoked only on the primary Administration Server.

To revoke a EULA for managed Kaspersky applications:

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab of the Administration Server properties window, go to the **End User License Agreements** section.

   A list of EULAs—accepted upon creation of installation packages or at the seamless installation of updates—is displayed.

3. 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
- Whether or not the EULA can be revoked

4. 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) linked to the EULA, and their respective names and types

5. In the lower part of the EULA properties window, click the **Revoke License Agreement** button.

   If the selected EULA can be revoked only by uninstalling the application or if this EULA can be revoked only on the primary Administration Server, a notification about this restriction is displayed instead of the **Revoke License Agreement** button.

   > If there exist any objects (installation packages and their respective tasks) that prevent the EULA from being revoked, the notification about it 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.

6. 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).

If the last license key is expired, Kaspersky Next Expert View automatically deletes your workspace after 90 days. As a result, you cannot manage the protection of your network by means of Kaspersky Next Expert View. You also permanently lose your data from Kaspersky Next Expert View. We recommend that you renew outdated license keys or add new ones to the Administration Server repository to keep your workspace.

To view a notification about an expired license or a license that is about to expire:

1. Do one of the following:

   - In the main menu, go to **Operations** → **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 the expiring and expired licenses.

2. If you want to renew a license, click the **Renew license** link next to the required license.

   By clicking a license renewal link, you agree to transfer the following data to Kaspersky: software ID, software version, software localization, license ID, and an attribute that shows if the license was provided by a partner company. The data is required to determine the renewal terms of your license.

3. In the window of the license renewal service that opens follow the instructions to renew a license.

   The license is renewed.

In Kaspersky Next Expert View, 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

Use of Kaspersky Next Expert View after the license expiration

After the license expiration, Kaspersky might grant you the use of Kaspersky Next Expert View for up to 90 days without limitations. During this period, the Administration Server, Network Agent, and Kaspersky Next Expert View web interface work without limitations. Kaspersky Next Expert View also sends KSN statistics to Kaspersky in accordance with the current KSN access settings. The managed applications work with only limited functionality (for details, refer to the documentation for these applications).

When the license has been expired for 90 days, Kaspersky Next Expert View automatically deletes your workspace. If you want to keep the workspace, renew at least one expired license key or add a new one to the repository.

Licensing definitions

This section contains definitions for concepts related to licensing of Kaspersky applications managed via Kaspersky Next Expert View.

About the license

A *license* is a time-limited right to use Kaspersky Next Expert View, 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 Next Expert View 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 Next Expert View 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.

About the activation code

An *activation code* is a unique sequence of twenty Latin letters and numerals. You enter an activation code to add a license key that activates Kaspersky Next Expert View. You receive the activation code through the email address that you specified after purchasing Kaspersky Next Expert View or after ordering the trial version of Kaspersky Next Expert View.

To activate the application by using the activation code, you need internet access in order to connect to Kaspersky activation servers. If access to the servers using system DNS is not possible, the application uses public DNS servers.

If the application was activated with an activation code, the application in some cases sends regular requests to Kaspersky activation servers in order to check the current status of the license key. You must provide the application internet access to make it possible to send requests.

If you have lost your activation code after installing the application, contact the Kaspersky partner from whom you purchased the license.

> You cannot use key files for activating managed applications; only activation codes are accepted.

About the subscription

Subscription to Kaspersky Next Expert View 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 Next Expert View 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 Next Expert View 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 Next Expert View under subscription, you must apply the activation code received from the service provider.

You can apply a different activation code for Kaspersky Next Expert View 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 Next Expert View.

When the application is used under subscription, Kaspersky Next Expert View 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.

Data provision

Kaspersky Next Expert View enables the user to identify and control devices (and the device owners) connected to Kaspersky Next Expert View, by means of the features of managed applications.

Data provision methods:

1. The User enters data in the Kaspersky Next Expert View interface.

2. Network Agent receives data from the device and transfers it to Administration Server.

3. Network Agent receives data retrieved by the Kaspersky managed application and transfers it to Administration Server. The list of data processed by Kaspersky managed applications is provided in the Help of the corresponding applications.

4. Data is transferred from secondary Administration Servers running on-premises.

Kaspersky Next Expert View automatically deletes workspaces 30 days after the trial license term expires, 90 days after the commercial license term expires.

After the license term expires, Kaspersky saves User's data related to alerts and incidents in the User's workspaces for 30 days.

Under the current license, the storage term for alerts and for incidents is 360 days. After this period, the older alerts and the older incidents are automatically deleted.

The final deletion of the data listed in this section may take up to 24 hours.

Data sent to Kaspersky servers

Data sent during activation

When using the Activation Code to activate Software, in order to verify the legitimacy of using the software, the User agrees to periodically provide Kaspersky with the following information:

- Activation code

- Unique activation identifier for the current license

Kaspersky can also use this information to generate statistical information about the distribution and use of Kaspersky software.

Data sent during updating

Upon receipt of Updates from the Rightholder's update servers, in order to improve the quality of the update mechanism, the User agrees to periodically provide the following information to Kaspersky:

- Software ID received from the license
- Full version of the software
- Software license ID
- Software installation ID (PCID)
- ID of the software update startup

Kaspersky can also use this information to generate statistical information about the distribution and use of Kaspersky software.

Data for ensuring uninterrupted operation, efficient work, and verifying the legitimate use of Kaspersky Next Expert View

The following information can be used for the specified purpose:

- Names and versions of Kaspersky security applications connected to the workspace, as well as number of devices on which these security applications are installed.
- Number of devices with Kaspersky security applications installed that have been connected to all workspaces and distribution of these connected devices by type.
- Workspace identifier, workspace country and region, and workspace creation date.
- Number of users in the workspace, date of the last authentication in the workspace.
- Details of the currently used license (license type, license limit on the number of devices, number of connected devices, and expiration date of the previously used license).

Data transferred when following the links in the interface of Kaspersky Next Expert View

Following the links in the Administration Console or Kaspersky Next Expert View, the User agrees to the automatic transfer of the following data:

- Localization of Kaspersky Next Expert View
- License ID
- 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.

Data necessary for the functioning of managed applications

The following managed applications transfer data from the device to Administration Server through Network Agent:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent
- Kaspersky Endpoint Security for Android
- Kaspersky Security for iOS
- Kaspersky Secure Mobility Management
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux

The list of processed data is published in the Data Processed by Kaspersky Next When Connecting Devices Agreement.

User data processed locally

The only Kaspersky Security Center component that can be deployed locally in a Kaspersky Next Expert View is Network Agent.

User data list processed locally:

- All data listed in the User Data section processed within the framework and infrastructure of Kaspersky, except for data that the administrator enters through the Kaspersky Next Expert View interface
- Kaspersky Event Log of Network Agent
- Traces of Network Agent
- Logs, including logs created by the Network Agent installer, Kaspersky Security Center utilities

The dump, log, and trace files of Network Agent contain random data and may contain personal data. Files are stored unencrypted on the device on which Network Agent is installed. Files are not transferred to Kaspersky automatically. The user can transfer this data to Kaspersky manually at the request of the Technical Support to solve problems in the operation of Kaspersky Security Center.

About legal documents of Kaspersky Next Expert View

To use Kaspersky Next Expert View, you must read and express your agreement with the terms and conditions of the legal documents specified on the Kaspersky Next Expert View website. You can view the terms and conditions of AO Kaspersky Lab Privacy Policy for websites when you sign in to Kaspersky Next Expert View to manage a workspace. You can read Kaspersky Next Expert View Agreement and Kaspersky Next Expert View Data Processing Agreement when you create a company workspace.

Please carefully read the texts of all the legal documents before you start using Kaspersky Next Expert View.

End User License Agreement for Kaspersky applications

The End User License Agreement (hereinafter also referred to as License Agreement or EULA) is a binding agreement between you and AO Kaspersky Lab stipulating the terms under which you may use the Kaspersky applications.

You can familiarize yourself with the terms of the End User License Agreement in the following ways:

- In the window which is displayed during Kaspersky application installation package creation.
- In the license.txt file, in the Kaspersky application installation folder, on the managed device.

You can revoke your acceptance of the End User License Agreement at any time.

If you do not accept the terms of the License Agreement for a Kaspersky application, you cannot use this application.

Hardening Guide

Kaspersky Next Expert View 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 Next Expert View allows you to configure all components of protection built by using Kaspersky applications.

Kaspersky Next Expert View 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 Next Expert View 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 Next Expert View 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

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 Next Expert View 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 Next Expert View, 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.

Administration Server location

Devices managed by Administration Server can be located as follows:

- On a local area network (LAN)
- On the internet
- In the demilitarized zone (DMZ)

At the same time, Administration Server can also be located in different segments: industrial, corporate, and DMZ segments.

If you use Kaspersky Next Expert View to manage protection of an isolated network segment, we recommend deploying Administration Server in a segment of the demilitarized zone (DMZ). This allows you to organize a proper network segmentation and minimize traffic flow to the protected segment, while maintaining full management capabilities and update delivery.

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.

For example, security restrictions usually applied to a domain controller can significantly reduce the performance of Administration Server and make it impossible to use some features of Administration Server. If an intruder gains privileged access to the domain controller, Active Directory Domain Services (AD DS) database can be modified, damaged, or destroyed. Also, all systems and accounts managed by Active Directory can be compromised.

Accounts for installing and running Administration Server

We recommend running the Administration Server installation under a local administrator account to avoid using domain accounts to access the Administration Server database. A set of the required accounts and their rights depends on the selected DBMS type, DBMS location and method of the Administration Server database creation.

The KLAdmins and KLOperators groups are created automatically during Kaspersky Next Expert View installation. These groups are granted permissions to connect to the Administration Server and to process Administration Server objects.

Depending on the type of account that is used for installation of Kaspersky Next Expert View, the KLAdmins and KLOperators groups are created as follows:

- If the application is installed under a user account included in a domain, the groups are created on the Administration Server device and in the domain that includes Administration Server.
- If the application is installed under a system account, the groups are created on the Administration Server device only.

In order to avoid creating the KLAdmins and KLOperators groups in the domain and, as a result, **providing privileges to manage Administration Server to an account outside the Administration Server device**, we recommend installing Kaspersky Next Expert View under a local account.

During Administration Server installation, select the account that will be used to start Administration Server as a service. By default, the application creates a local account named KL-AK-*, under which the Administration Server service (the klserver service) will run.

If necessary, the Administration Server service can be run under the selected account. This account must be granted the required rights to access the DBMS. For security reasons, use a non-privilege account to run the Administration Server service.

To avoid the use of incorrect account settings, we recommend generating the account automatically.

Excluding Administration Server from a domain

If you use Administration Server to protect device groups of high-importance systems, we do not recommend including the Administration Server device in the domain. This allows you to differentiate Kaspersky Next Expert View management rights and prevent access to Administration Server in case the domain account is compromised.

Take into account that if you install Administration Server on a device included in the workgroup, the following scenarios of working with Administration Server will not be available:

- Using a Kaspersky Next Expert View failover cluster
- Using a Windows Server failover cluster
- Using SQL Server for Windows on a separate device

  You can use SQL Server for Windows on a separate device only if Administration Server and SQL Server are in the same domain or trusted domains. If Administration Server, SQL Server and a UNC share for backups are in a workgroup, you cannot securely set up access and read-write rights between the SQL Server and the share.
- Remote installation with Administration Server tools through Active Directory group policies

If you need to disconnect the Administration Server from the Active Directory domain, follow the steps described in the article How to change the name of the Kaspersky Next Expert View.

If it is necessary to install Administration Server on a device included in the workgroup, you can also use Kaspersky Security Center Linux instead of Kaspersky Security Center Windows.

Accounts and authentication

Before following these steps, create a backup copy of Kaspersky Next Expert View 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 Next Expert View provides two-factor authentication for users of Kaspersky Next Expert View and Administration Console, based on the RFC 6238 standard (TOTP: Time-Based One-Time Password algorithm).

When two-step verification is enabled for your own account, every time you log in to Kaspersky Next Expert View or Administration Console, you enter your user name, password, and an additional single-use security code. If you use domain authentication for your account, you only have to enter an additional single-use security code. To receive a single-use 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.

Restricting new users from setting up two-step verification for themselves

In order to further improve Kaspersky Next Expert View access security, you can

prohibit new users from setting up two-step verification for themselves.

If this option is enabled, a user with disabled two-factor authentication, for example new domain administrator, cannot configure two-factor authentication for themselves. Therefore, such user cannot be authenticated on Administration Server and cannot sign in to Kaspersky Next Expert View without approval from another Kaspersky Next Expert View administrator who already has two-step verification enabled.

Using two-factor authentication for an operating system

We recommend using multi-factor authentication (MFA) for authentication on the Administration Server device by using a token, a smart card, or other method (if possible).

Prohibition on saving the administrator password

If you use Administration Console, we do not recommend saving the administrator password in the Administration Server connection dialog box.

If you use Kaspersky Next Expert View, 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 Next Expert View 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.

The KLAdmins and KLOperators groups

The KLAdmins and KLOperators groups are created automatically during Kaspersky Next Expert View installation. The KLAdmins group is granted all access rights. The KLOperators group is granted only Read and Execute rights. The rights granted to the KLAdmins group are **locked**.

You can view the KLAdmins and KLOperators groups, and make changes to these groups, by using the standard administrative tools of the operating system.

When developing regulations for working with Administration Server, it is necessary to determine whether the information security specialist needs full access (and inclusion in the KLAdmins group) to perform standard tasks.

Most of the basic administration tasks can be distributed between company departments (or different employees of the same department) and consequently between different accounts. You can also set up administration groups access differentiation in Kaspersky Next Expert View. As a result, it is possible to implement a scenario in which authorization under accounts from the KLAdmins group will be anomalous and could be considered an incident.

If Kaspersky Next Expert View was installed under a system account, groups are created only on the Administration Server device. In this case, we recommend making sure that only entries created during the installation of Kaspersky Next Expert View are included in the group. We do not recommend adding any groups to the KLAdmins group (local and/or domain) that is created automatically during the Kaspersky Next Expert View installation. You should also limit the rights to change this group. The KLAdmins group must include only single unprivileged accounts.

If the installation was performed under a domain user account, groups KLAdmins and KLOperators are created both on Administration Server and in the domain that includes Administration Server. A similar approach such as local account installation is recommended.

Restricting the Main Administrator role membership

We recommend restricting the Main Administrator role membership.

By default, after the Administration Server installation, the Main Administrator role is assigned to the local administrators group and the created KLAdmins group. It is useful for management, but it is critical from a security point of view, because the Main Administrator role has an extensive range of privileges, the assignment of this role to users should be strictly regulated.

Local administrators can be excluded from the list of users with administrator privileges of Kaspersky Next Expert View. The Main Administrator role cannot be removed from the KLAdmins group. You can include in the KLAdmins group the accounts that will be used to manage Administration Server.

If you use domain authentication, we recommend restricting the privileges of domain administrator accounts in Kaspersky Next Expert View. By default, these accounts have the Main Administrator role. Also, a domain administrator can include its account in the KLAdmins group to obtain the Main Administrator role. To avoid this, in the Kaspersky Next Expert View security settings you can add the Domain Admins group, and then define prohibiting rules for it. These rules must take precedence over the allowing ones.

You can also use the predefined user roles with an already configured set of rights.

Configuring access rights to application features

We recommend using flexible configuration of access rights to the features of Kaspersky Next Expert View 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.

Securing Windows Privileged Access

We recommend taking into account Microsoft's recommendations for providing privileged access security. To view these recommendations, go to the Securing privileged access article.

One of the key points of recommendations is the implementation of Privileged Access Workstations (PAW).

Using a managed service account (MSA) or a group managed service accounts (gMSA) to run the Administration Server service

Active Directory has a special type of accounts for securely running services, called group Managed Service Account (MSA/gMSA). Kaspersky Next Expert View supports managed service accounts (MSA) and group managed service accounts (gMSA). If these types of accounts are used in your domain, you can select one of them as the account for the Administration Server service.

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 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 may be compromised because the shared Read access rights are enabled to the repository of installation packages.

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 Next Expert View users

Special security requirements must be applied to Kaspersky Next Expert View users' devices. We recommend protecting these devices against any type of unauthorized access (including physically):

Kaspersky Next Expert View user devices include the following:

- Devices from which users connect to Kaspersky Next Expert View by using a browser.
- Devices from which users connect to Kaspersky Next Expert View by using the MMC-based Administration Console.
- Devices from which applications that interact with Administration Server via OpenAPI are connected to Kaspersky Next Expert View.

Security requirements for devices with Kaspersky Next Expert View installed

Devices with Kaspersky Next Expert View installed are used to manage Kaspersky Next Expert View, 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 Kaspersky Next Expert View applications and for all components that you use (Network Agent, Kaspersky Endpoint Security for Windows, 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

To prevent intruders from disabling Kaspersky security applications, we strongly recommend enabling password protection for disabling protection and deinstallation of Kaspersky security applications. You can set the password, for example, for Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Servers, Network Agent, and other Kaspersky applications. After you enable password protection, we recommend locking these 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. When Network Agent is installed on a client device, the utility is automatically copied to 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. Password protection for running the klmover utility can be omitted for devices operated without local administrator rights.

Enabling the **Use uninstallation password** option 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 Active Directory 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.

Selecting a shared folder

If you deploy Administration Server on the device running Windows with the selection of an existing shared folder (that is used, for example, for placing installation packages and storage of updated databases), we recommend ensuring that read rights are granted to the Everyone group, and write rights are granted to the KL Admins group.

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 Next Expert View 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.

Statistics of the Administration Server function

For timely response to security issues, we recommend configuring the sending of statistics of the Administration Server function to third-party applications, by using Simple Network Management Protocol (SNMP).

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

Multiple users with different levels of computer literacy can share a device with Kaspersky Endpoint Security for Windows installed. If users have unrestricted access to Kaspersky Endpoint Security for Windows and its settings, the overall level of device protection may be reduced. Password protection allows you to restrict users' access to Kaspersky Endpoint Security for Windows, according to the permissions granted to them (for example, permission to exit the application).

One of the ways to restrict access to Kaspersky Endpoint Security for Windows and its parameters is to use a KLAdmin account. 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. 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.

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.

Interface of Kaspersky Next Expert View

Kaspersky Next Expert View is managed through the web interface.

The application 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. Click the Administration Server name to open the Administration Server properties.
- **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, the **Console navigation** section 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 to manage client devices, as well as tasks and Kaspersky application policies.
- **Users & roles**. Allows you to manage users and roles, configure user rights by assigning roles to the users, and associate policy profiles with roles.
- **Operations**. Contains a variety of operations, including application licensing, patch management, and third-party application management. This also provides you access to application repositories.
- **Discovery & deployment**. Allows you to poll the network to discover client devices, and distribute the devices to administration groups manually or automatically. This 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**. Contains settings to integrate Kaspersky Next Expert View with other Kaspersky applications. It also 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 Next Expert View home page opens.

The center of the pane contains the drop-down list with the name of your current workspace. If you click the drop-down list and select one of the items, you can do one of the following:

- Switch to another workspace, if it is available.
- Return to the list of workspaces.

On the right side of the pane, the menu of your account is displayed. You can open the menu by clicking your account name, and then do one of the following by selecting the corresponding item from the drop-down list:

- Manage your account settings.

  If you select the **Manage user account** item, you are redirected to the Kaspersky Account portal, where you can change your password or email address, as well as set up two-factor authentication.
- Select the language of Kaspersky Next Expert View interface.
- Select the light mode of the interface.
- View the information about Kaspersky Technical Support.
- Move to Kaspersky Next Expert View Help.
- Watch tutorial videos on how to configure and use Kaspersky Next Expert View and security applications.

  In the Mozilla Firefox browser, if you play a video in the **Tutorials** section in the pop-up window, then open the video in the picture in picture mode, and then close the video in the pop-up window, the video in the picture in picture mode is closed as well.
- View the information about legal documents for Kaspersky software available to you.
- Sign out of Kaspersky Next Expert View.

Work area

The work area displays the information you choose to view in the sections of the application web interface window. It also contains control elements that you can use to configure how the information is displayed.

Changing the language of the Kaspersky Next Expert View interface

You can select the language of the Kaspersky Next Expert View 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 Kaspersky Next Expert View home page

The home page is displayed after you sign in to Kaspersky Next Expert View.

By default, the **Home page settings** tab of 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.

Pinning and unpinning sections of the main menu

You can pin sections of Kaspersky Next Expert View to add them to favorites and access them quickly from the **Bookmarks** section in the main menu.

If there are no pinned elements, the **Bookmarks** section is not displayed in the main menu.

You can pin sections that display pages only. For example, if you go to **Asset management** → **Assets (Devices)**, a page with the table of devices opens, which means you can pin the **Assets (Devices)** section. If a window or no element is displayed after you select the section in the main menu, then you cannot pin such a section.

To pin a section:

1. In the main menu, hover the mouse cursor over the section you want to pin.

   The pin icon (📌) is displayed.

2. Click the pin icon (📌).

The section is pinned and displayed in the **Bookmarks** section.

You can also remove elements from favorites by unpinning them.

To unpin a section:

1. In the main menu, go to the **Bookmarks** section.
2. Hover the mouse cursor over the section you want to unpin, and then click the unpin icon (📌).

The section is removed from favorites.

Returning to the list of workspaces

After opening the workspace, you can go back to the portal page, which displays the workspaces you have created. If administrators of other workspaces have granted you access by assigning the Viewer or Administrator role to your account, those workspaces will also appear on your portal page.

To return to the list of workspaces:

1. In the upper pane, click the drop-down list with the name of your current workspace.
2. Select **Go to portal**.

The portal page displays the list of workspaces.

Initial configuration of Kaspersky Next Expert View

This section outlines the main scenario for Kaspersky Next Expert View deployment starting with a workspace creation and finishing with the monitoring of the network protection status.

For information about deployment of Kaspersky Security Center running on-premises, refer to Kaspersky Security Center Help.

We recommend that you assign a minimum of one working day for completion of this scenario.

The scenario guides you through the following:

- Starting work with a workspace as an administrator
- Discovering devices on your network (if necessary, you will assign distribution points and manually install distribution packages on them)
- Deploying managed Kaspersky applications on the client devices; configuring tools for network protection, monitoring, and regular updates of Kaspersky databases, software modules, and applications

When you complete this scenario, the network protection based on Kaspersky applications will be configured. You will be able to proceed to monitoring of the network protection status.

Prerequisites

Before you start:

- View the architecture of Kaspersky Next Expert View to understand interaction between the main application components.
- Read information about the licensing of Kaspersky Next Expert View and managed applications.
- Make sure that you have a valid activation code for Kaspersky Next Expert View (if you are creating a commercial workspace).

Stages

Kaspersky Next Expert View configuration proceeds in stages:

1. **Configuring ports**

   Make sure that all necessary ports are open for interaction between your network and the Kaspersky infrastructure. Also, if you plan to use the hierarchy of Administration Servers, make sure that all necessary ports are open for interaction involving the secondary Administration Server (or secondary Administration Servers) and client devices.

2. **Creating a workspace**

   Create an account, and then create a workspace.

3. **Running quick start wizard**

   Open and sign in to Kaspersky Next Expert View. When you sign in for the first time, you are automatically prompted to run the quick start wizard. You can also start the quick start wizard manually at any time.

   When the quick start wizard is complete, you will have installation packages of Network Agent and security applications. These installation packages are required for further deployment of Kaspersky Next Expert View.

4. **Deploying Kaspersky applications**

   Perform the scenario of initial deployment of Kaspersky applications. One of the scenario steps refers to the network polling operation. This operation is required to discover client devices of your network. Network polling and its settings are described in the scenario of discovering networked devices.

5. **Licensing Kaspersky security applications**

   When Kaspersky security applications are deployed to the managed devices, the applications must be licensed by applying an activation code to each of the applications. Deploy your activation codes to the Kaspersky applications installed on the managed devices. You have several options to license Kaspersky security applications.

6. **Configuring network protection**

   Perform the network protection configuration to fine-tune the policies and tasks created through the quick start wizard. Pay attention to optimizing the load on endpoint protection applications.

7. **Regular updating of Kaspersky databases, software modules, and applications**

   To keep your network protected against viruses and other threats, you have to configure regular updates of Kaspersky databases, software modules, and applications.

8. **Updating third-party software and fixing third-party software vulnerabilities (optional)**

   Kaspersky Next Expert View enables you to manage updates of Microsoft applications installed on client devices. You can also fix vulnerabilities in Microsoft applications through installation of required updates.

9. **Configuring tools for monitoring the network protection status**

   Select and configure widgets, reports and other tools that allow you to monitor the network protection status.

When Kaspersky Next Expert View is deployed and configured, you can proceed to monitoring the network protection status.

Scenario: Creating a hierarchy of Administration Servers managed through Kaspersky Next Expert View

This scenario describes the actions that you must perform to create a hierarchy of Administration Servers managed through Kaspersky Next Expert View, which thus assumes the role of primary Administration Server. This hierarchy can be subsequently used for migration of managed devices and objects from Kaspersky Security Center to Kaspersky Next Expert View, as well as management of secondary Administration Servers and devices through Kaspersky Next Expert View.

Kaspersky Next Expert View can only act as primary Administration Server, while Administration Servers running on-premises can only act as secondary Administration Servers. Other hierarchical schemes are not available.

Prerequisites

Make sure that the following prerequisites are met:

- Upgrading Administration Server running on-premises to version 12 or later.
- Installing Kaspersky Security Center Web Console on the Administration Server running on-premises.
- Installing the web plug-ins for the applications that you intend to manage through Kaspersky Next Expert View.
- Upgrading the managed applications to versions supported by Kaspersky Next Expert View.
- Making sure that the Download updates to the Administration Server repository task on the Administration Server running on-premises does not have the primary Administration Server assigned as the update source; modifying the task settings accordingly, if necessary.

After the hierarchy is created, the policies and tasks that are effective in Kaspersky Next Expert View are applied on the secondary Administration Server, thus superseding its existing policies and tasks. If you want to avoid this behavior, delete all policies and tasks of Kaspersky Next Expert View before the hierarchy creation. Alternatively, you can change the status of each Kaspersky Next Expert View policy to **Inactive** in its settings and disable the **Distribute to secondary and virtual Administration Servers** option in the settings of each Kaspersky Next Expert View task.

You can delete your hierarchy of Administration Servers at any time, if necessary.

Stages of hierarchy creation

The basic scenario provides for a secondary Administration Server that cannot be accessed over the internet. However, the set of actions within some of the steps described below may vary if the secondary Administration Server is accessible over the internet. Also, some of the steps must be skipped in this case.

Creation of a hierarchy of Administration Servers comprises the following stages:

1. **Retrieving the certificate of the secondary Administration Server**

   If the secondary Administration Server is accessible over the internet, skip this step.

   In Kaspersky Security Center Web Console running on-premises, open the Administration Server properties and on the **General** tab, open the **General** section. Click the **View Administration Server certificate** link. The certificate file, in the CER format, is automatically saved in the folder specified in your browser settings.

2. **Retrieving the connection settings and certificates from Kaspersky Next Expert View**

   If the secondary Administration Server is accessible over the internet, skip this step.

   In Kaspersky Next Expert View, open the Administration Server properties and on the **General** tab open the **Hierarchy of Administration Servers** section. The following connection settings are displayed:

   - **HDS address**

     Displays the web address used for connection to Hosted Discovery Service (HDS).

   - **HDS port**

     Displays the number of the port used for connection to HDS.

   The section also contains two links:

   - **View Administration Server certificate**

     Clicking this link starts the download of the public key of the Kaspersky Next Expert View instance certificate.

   - **HDS Root CA certificate**

     Clicking this link starts the download of the file in .pem format that contains a list of trusted root certificates issued by Certification Authorities (CA). This file is designed for use by the secondary Administration Server: it is required to verify the HDS certificate.

   Copy the connection settings manually—by using the clipboard or any other convenient way—and save them to a file of any convenient format. Click the **View Administration Server certificate** link and wait until the certificate file is downloaded. Click the **HDS Root CA certificate** link and wait until the file with the list of trusted root certificates issued by Certification Authorities is downloaded. Both files are saved to the folder specified in your browser settings.

3. **Selecting the secondary Administration Server for connection**

In the Administration Server properties, proceed to the **Administration servers** tab. In the hierarchy of administration groups, select the check box next to the administration group that you want to contain the secondary Administration Server with all its managed devices. Click the **Connect secondary Administration Server** button.

On the page that opens, in the **Secondary Administration Server display name** field specify the name under which the secondary Administration Server must be displayed in the hierarchy. It is used for your convenience only and so it can differ from the actual secondary Administration Server name, if necessary. Click **Next**.

If the secondary Administration Server is accessible over the internet, you must also specify the address of the secondary Administration Server in the **Secondary Administration Server address (optional)** field.

On the next page, click the **Browse** button and specify the .pem file that you saved from the secondary Administration Server. Click **Next**.

4. **Enabling and configuring proxy server**

The actions described in this step are optional. Perform them only if your connection requires the use of proxy server.

Click **Next**. On the **Connection and authentication settings** page, you can enable and configure the use of proxy server, if necessary. Select the **Use proxy server** check box and specify the following proxy settings:

- **Proxy server address**

  Address of the proxy server.

- **User name**

  The user name to log in to the proxy server.

- **Password**

  The password to log in to the proxy server.

5. **Specifying the authentication settings and adding the secondary Administration Server to the hierarchy**

Click **Next**. On the **Secondary Administration Server credentials** page, specify the following settings:

- **User name**

  The user name under which you log in to the secondary Administration Server.

- **Password**

  The password used to log in to the secondary Administration Server.

Click **Next** and wait until the secondary Administration Server appears in the hierarchy.

If the secondary Administration Server is accessible over the internet, it connects to the primary Administration Server.

If the secondary Administration Server is accessible over the internet and the connection between the two Administration Servers is successfully established, skip all further steps.

If the secondary Administration Server cannot be accessed over the internet, it becomes visible but you must perform additional actions on the secondary Administration Server to gain control of it.

6. **Configuring the connection in Kaspersky Security Center Web Console running on-premises**

In Kaspersky Security Center Web Console running on-premises, open the Administration Server properties and on the **General** tab, open the **Hierarchy of Administration Servers** section. Select the **This Administration Server is secondary in the hierarchy** check box. In the **Type of primary Administration Server** list, select the **Kaspersky Security Center Cloud Console** option.

Kaspersky Security Center Web Console checks whether the primary Administration Server is specified as the update source in the *Download updates to the Administration Server repository* task. If the primary Administration Server is specified as the update source, you get the corresponding warning message and a link to the task settings. You can modify the settings and then go back to the hierarchy creation, or you can skip this action and proceed with the hierarchy creation.

In the **Settings to establish connection between secondary and primary Administration Servers** group, specify the following settings:

- **HDS server address (from primary Administration Server on Cloud Console)**

  Enter the address of the HDS server in Fully Qualified Domain Name (FQDN) format, which you have copied and saved from the Administration Server properties in Kaspersky Next Expert View.

- **HDS server ports**

  Enter the number(s) of the HDS server port(s), which you have copied and saved from the Administration Server properties in Kaspersky Next Expert View.

7. **Adding the certificates to the secondary Administration Server**

Click the **Specify primary Administration Server certificate** button and specify the certificate file that you saved from the Administration Server properties in Kaspersky Next Expert View.

Click the **Specify Hosted Discovery Service certificates** button and specify the .pem file that you saved from the Administration Server properties in Kaspersky Next Expert View.

If you have enabled the use of proxy server when connecting the secondary Administration Server in Kaspersky Next Expert View, select the **Use proxy server** check box and specify the same proxy settings as in Kaspersky Next Expert View.

You can also select the **Connect primary Administration Server to secondary Administration Server in DMZ** check box if the secondary Administration Server is in a demilitarized zone (DMZ).

The secondary Administration Server connects to the primary Administration Server.

Results

Upon performing the above steps, you can make sure that the hierarchy is created successfully:

- The active policies of the primary Administration Server become effective on the secondary Administration Server. The tasks of the primary Administration Server are distributed to the secondary Administration Server. If the **Distribute to secondary and virtual Administration Servers** option is enabled in the settings of a group task, every such task is also distributed to the secondary Administration Server.
- Policy settings that are locked against changes on the primary Administration Server are displayed as locked against changes in all policies on the secondary Administration Server.
- Policies applied by the primary Administration Server are displayed in the list of policies of the secondary Administration Server (**Asset management** → **Policies**).
- Group tasks distributed by the primary Administration Server are displayed in the list of tasks of the secondary Administration Server (**Asset management** → **Tasks**).
- Policies and tasks created on the primary Administration Server cannot be modified on the secondary Administration Server.
- In Kaspersky Next Expert View, in the structure of administration groups the secondary Administration Server is displayed within the group that you selected when you added this Administration Server.

Migration to Kaspersky Next Expert View

This section describes the process of migration from Kaspersky Security Center of version 12 (or later) running on-premises to Kaspersky Next Expert View.

Migration from Kaspersky Security Center Linux to Kaspersky Next Expert View is not supported.

Methods of migration to Kaspersky Next Expert View

By using the migration feature, you can transfer your networked devices from Kaspersky Security Center under management by Kaspersky Next Expert View. Your managed devices will be switched without losing the principal settings, such as membership in administration groups; as well as the essential objects, such as policies and tasks related to the managed applications.

You can choose either of the two available methods to migrate your Administration Servers to Kaspersky Next Expert View:

- Migration without a hierarchy of Administration Servers:
  - Enables transfer of managed devices and related objects to Kaspersky Next Expert View, even if the Administration Server on-premises is not secondary in regard to Kaspersky Next Expert View.
  - May require transfer of files (on a removable drive, by email, through shared folders, or in any other convenient way) if Kaspersky Security Center Web Console and Kaspersky Next Expert View are opened on different physical devices.

  You can also perform migration with virtual Administration Servers if your network includes them.
- Migration using a hierarchy of Administration Servers:
  - Enables transfer of managed devices and related objects to Kaspersky Next Expert View by using only the interface of Kaspersky Next Expert View, so no physical transfer of files is needed.
  - Requires that the Administration Server running on-premises act as secondary to Kaspersky Next Expert View. You can create such a hierarchy before starting migration.

For the full disk encryption, Kaspersky Next Expert View supports only BitLocker.

Scenario: Migration without a hierarchy of Administration Servers

This section describes the migration of the managed devices and related objects (such as policies, tasks, reports) from Kaspersky Security Center Web Console running on-premises to Kaspersky Next Expert View. You can include a single administration group in the migration scope to restore the same administration group in Kaspersky Next Expert View.

This group must contain the managed devices of a single operating system. If your network includes the devices of different operating systems or Linux distributives, allocate them in different administration groups, and then migrate each group separately.

After you finish the migration, all Network Agents within the migration scope are upgraded and managed by Kaspersky Next Expert View.

> The steps listed in this section cover the migration process performed when no hierarchy of Administration Servers exists, that is, no connection has been established between Kaspersky Next Expert View and Kaspersky Security Center Web Console running on-premises.

Prerequisites

Before you start, do the following:

- Upgrade Administration Server running on-premises to version 14.2 or later.
- Install Kaspersky Security Center Web Console version 12.1 or later.
- Upgrade Network Agent on managed devices to version 12 or later.
- On Windows devices, use Network Agent without an uninstallation password.

  If the password has already been set, do one of the following in Kaspersky Security Center Web Console:

  - Disable the **Use uninstallation password** option in the Network Agent policy settings.
  - Uninstall Network Agent remotely by using the *Uninstall application remotely* task. In the **Application to uninstall** field of the task, select **Kaspersky Security Center Network Agent**. Do not forget to enter the uninstallation password.
- Upgrade the managed applications to the versions supported by Kaspersky Next Expert View.
- Make sure that you have policies for the latest versions of the managed applications. If you use outdated policies, create new ones for the application versions supported by Kaspersky Next Expert View.
- To use actual policies, upgrade the web plug-ins for the applications that you intend to manage through Kaspersky Next Expert View.

- Uninstall Kaspersky applications from managed devices if these applications are not supported by Kaspersky Next Expert View.
- Decrypt all the data (disk-level or file-level) that was encrypted by Kaspersky Endpoint Security for Windows on managed devices running the Windows operating system, and disable the encryption feature on the managed devices through the application policy or locally. For more information, see Help for Kaspersky Endpoint Security for Windows.

  If the Windows device still stores any files or folders encrypted through Kaspersky Endpoint Security for Windows, the Network Agent upgrade will be canceled during the migration process. A notification will prompt you to decrypt all data on the device and disable the encryption feature.

Kaspersky Next Expert View allows for a maximum of 25,000 managed devices per one Administration Server.

Migration stages

Migration to Kaspersky Next Expert View comprises the following stages:

1. **Planning the migration scope and checking the prerequisites**

   Estimate the scope of the migration process, that is, review the administration group to export and assess the number of managed devices in it. Also, make sure that all the activities listed as migration prerequisites have been completed successfully.

2. **Exporting managed devices, objects, and settings from Kaspersky Security Center Web Console**

   Use the Migration wizard of Kaspersky Security Center Web Console running on-premises to export your managed devices together with their objects.

   The maximum export file size is 4 GB.

3. **Importing the export file to Kaspersky Next Expert View**

   Transfer the information about your managed devices and objects to Kaspersky Next Expert View. For this purpose, use the Migration wizard of Kaspersky Next Expert View to import the export file and create a Network Agent stand-alone installation package.

4. **Re-installing Network Agent on managed devices**

   Go back to the Migration wizard in Kaspersky Security Center Web Console running on-premises to create a remote installation task. You will be able to use this task (immediately or later) to re-install Network Agent on your managed devices and complete the migration process.

Results

Upon finishing with the migration, you can make sure that it was successful:

- Network Agent is re-installed on all managed devices.
- All devices are managed through Kaspersky Next Expert View.
- All object settings that were effective before migration are preserved.

Migration wizard

This section provides information about the Migration wizard in Kaspersky Next Expert View and Kaspersky Security Center Web Console of version 12 or later.

Step 1. Exporting managed devices, objects, and settings from Kaspersky Security Center Web Console

Migration of managed devices from Kaspersky Security Center Web Console to Kaspersky Next Expert View requires that you first create an export file containing information about the hierarchy of administration groups that are on your current Administration Server running on-premises. The export file must also contain information about the objects and their settings. The export file will be used for subsequent import to Kaspersky Next Expert View.

The maximum export file size is 4 GB.

To export objects and their settings from Kaspersky Security Center Web Console:

1. In the main menu of Kaspersky Security Center Web Console, go to **Operations** → **Migration**.
2. On the welcome page of the Migration wizard, click the **Next** button. This opens the **Managed devices to export**, which displays the entire administration group hierarchy of the corresponding Administration Server.
3. On the **Managed devices to export** page, click the chevron icon (>) next to the **Managed devices** group name to expand the hierarchy of administration groups. Select the administration group that you want to export.

   After migration from Kaspersky Security Center running on-premises to Kaspersky Next Expert View performed for two administration groups, the Remote installation tasks for these groups appear with the same name.

4. Select the managed applications whose policies and tasks must be transferred to Kaspersky Next Expert View together with group objects. To select the managed applications whose objects are to be exported, select the check boxes next to their names in the list.

Although Kaspersky Security Center Administration Server is present on the list, selecting the corresponding check box does not result in the export of its policies.

To make sure that your managed applications are supported by Kaspersky Next Expert View, click the corresponding link. It will redirect you to the Help article containing the list of applications managed by Kaspersky Next Expert View.

> If you select applications that are not supported by Kaspersky Next Expert View, the policies and tasks of these applications will be exported anyway and then imported, but you will not be able to manage them in Kaspersky Next Expert View due to unavailability of the dedicated plug-ins.

5. View the list of group objects exported by default and specify non-group objects to be exported together with the selected administration group, if necessary. Configure the export scope by including or excluding various objects, such as global tasks, custom device selections, reports, custom roles, internal users and security groups, and custom application categories. This page includes the following sections:

   - **Global tasks**

     The list of global tasks of managed applications, as well as global tasks of Network Agent.

     > If a global task that you selected applies to a specific object selection, this selection will also be exported.

     > Although the global tasks of Administration Server are present on the list, you cannot export them; selecting those tasks does not affect the export scope. Remote installation tasks also remain outside the export scope, because their respective installation packages cannot be exported.

   - **Device selections**

     The list of custom device selections.

   - **Reports**

     The editable list of report instances to be exported.

     > If a report that you selected applies to a specific object selection, this selection will also be exported.

     > Kaspersky Next Expert View contains the same set of report templates as Kaspersky Security Center Web Console, so you can select for export only the reports that you created manually or reconfigured.

   - **Group objects**

     The list of group objects to be exported by default. The following objects related to the selected administration group will be exported in their entirety by default:

     - Administration group structure, that is, all subgroups of the selected administration group.
     - Devices that have been included in the administration groups to be exported.

- Tags that have been assigned to the devices to be exported.

  If a tag was created in Kaspersky Security Center Web Console but never assigned to any device, it will not be exported. The auto-tagging rules will not be exported, either.

- Group policies of the managed applications that have been selected.

  Administration Server policies and Network Agent policies are not exported.

- Group tasks of the managed applications that have been selected and Network Agent group tasks.

  Administration Server tasks are not exported.

You can also prevent certain types of non-group objects from being exported:

- To cancel export for custom roles (that is, those created by the user only), select the **Exclude custom roles from export** check box.
- To cancel export for internal users and security groups, select the **Exclude internal users and security groups from export** check box.
- To cancel export for custom application categories with content added manually, select the **Exclude custom application categories from export** check box.

If you transfer devices of various operating systems to Kaspersky Next Expert View, non-group objects only need to be migrated once.

The Migration wizard checks the total number of managed devices included in the selected administration group. If this number exceeds 10,000, an error message appears. The **Next** button remains unavailable (dimmed) until the number of managed devices in the selected administration group falls within the limit.

6. After you defined the migration scope, click **Next** to start the export process. The **Creating the export file** page opens, where you can view the export progress for each type of object that you included in the migration scope. Wait until the refresh icons (↻) next to all items in the list of objects are replaced with green check marks (✓). The export process finishes and the export file is automatically downloaded to the default download location defined in your browser settings. The name of the export file appears in the lower part of the browser window.

7. When the **Export has completed successfully** page is displayed, proceed to the next stage performed in Kaspersky Next Expert View.

If you use Kaspersky Security Center Web Console and Kaspersky Next Expert View on different devices, you will have to copy the export file to a removable drive or choose other ways of transferring the file.

Step 2. Importing the export file to Kaspersky Next Expert View

To transfer information about managed devices, objects, and their settings that you exported from Kaspersky Security Center Web Console, you must import it to Kaspersky Next Expert View deployed in your workspace. This enables you to create a stand-alone installation package and use it for re-installation of Network Agent on your managed devices.

Before you start the Migration wizard in Kaspersky Next Expert View, make sure its current localization language is the same as the Kaspersky Security Center Web Console language during the export process. Switch the language, if necessary.

If you have previously completed the quick start wizard in your Kaspersky Next Expert View workspace, the **Managed devices** group includes policies and tasks created with the default settings. Delete these policies and tasks before importing the ones that you exported from Kaspersky Security Center Web Console.

To import the export file to Kaspersky Next Expert View:

1. In the main menu of Kaspersky Next Expert View, go to **Operations** → **Migration**.
2. On the welcome page of the Migration wizard, click **Import**. In the File Explorer window that opens, select the export file by browsing to the folder where it was saved, and click **Open**. Wait until the refresh icon (↻) next to the file uploading status is replaced with the green check mark (✓).
3. Click **Next**. The next page opens, displaying the entire hierarchy of administration groups of the Administration Server in Kaspersky Next Expert View.
4. Select the check box next to the target administration group to which the group objects must be restored and click **Next**. The Migration wizard displays a list of Network Agent installation packages available in Kaspersky Next Expert View.
5. Select the installation package containing the relevant version and localization of Network Agent and click **Next**.

   Select the Kaspersky Network Agent for Windows installation package only if you have previously completed the quick start wizard in your Kaspersky Next Expert View workspace and if you perform the migration of Windows devices.

   Wait until the Migration wizard creates a stand-alone installation package. The maximum file size of the stand-alone installation package for Network Agent is 200 MB.

   The file is unpacked and automatically downloaded to the default download location defined in your browser settings. The non-group objects and the group objects are restored to the target administration group.

   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 you have imported the entire **Managed devices** group, we recommend that you rename the newly imported subgroup to avoid confusion:

a. Go to the **Hierarchy of groups** section.

b. Click the name of the subgroup in the groups tree.

c. In the properties window that opens, in the **Name** field enter a different name (for example, "Migrated devices").

We recommend that you check whether the objects (policies, tasks, and managed devices) included in the export scope have been successfully imported to Kaspersky Next Expert View. To do this, go to the **Asset management** section and view whether the imported objects appear on the lists in the **Policies**, **Tasks**, and **Assets (Devices)** subsections.

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. After this, the devices start switching to Kaspersky Next Expert View.

6. Click **Finish** to close the Migration wizard window.

7. If you want to find and download the stand-alone installation package again, go to **Discovery & deployment** → **Deployment & assignment** → **Installation packages** and click the **View the list of stand-alone packages** button. In the list that opens, select the stand-alone installation package that you have created and click the **Download** button.

If you use Kaspersky Security Center Web Console and Kaspersky Next Expert View on different devices, you must copy the stand-alone installation package to a removable drive or choose other ways of transferring the file.

Step 3. Re-installing Network Agent on devices managed through Kaspersky Next Expert View

After you create the Network Agent stand-alone installation package, you can proceed to creation of a remote installation task. Performing this task enables you to re-install Network Agent on all managed devices so that these devices are switched under management through Kaspersky Next Expert View.

To reduce the risk of data loss, we recommend that you first perform the actions for a small administration group counting up to 20 managed devices located within the corporate network and including no physical servers. After finishing with these actions, check whether re-installation completed successfully and proceed to the full reinstallation scope.

To create a remote installation task and re-install Network Agent:

1. Go back to the Migration wizard in Kaspersky Security Center Web Console running on-premises.

We recommend using the Migration wizard to create a remote installation task to re-install Network Agent as described below. If it is necessary to use a custom remote installation task, you first need to manually create a custom installation package from the Network Agent stand-alone installation package. Please note that when creating a custom installation package, you must specify the "-s" key in the executable file command line. Otherwise, Network Agent reinstallation from this custom installation package completes with an error.

Depending on the current state of the Migration wizard, you can do one of the following:

- If you have not closed the Migration wizard after the export and your session has not expired, click the **Go to Step 3 of the Migration wizard** button. Select the **Upload stand-alone installation package** check box and click the **Select stand-alone installation package** button. In the browser window that opens, specify the Network Agent stand-alone installation package.

- If for any reason you need to run the Migration wizard again, select the **Upload stand-alone installation package** check box and click the **Select stand-alone installation package** button. In the browser window that opens, specify the Network Agent stand-alone installation package. After that, the Migration wizard again displays the hierarchy of administration groups of this Administration Server. Select the same group for which you created the export file and click **Next**.

  The Migration wizard checks again the total number of managed devices included in the selected administration group. If this number exceeds 10,000, an error message appears. The **Next** button remains unavailable (dimmed) until the number of managed devices in the selected administration group falls within the limit.

2. Wait until the stand-alone installation package is uploaded and click **Next**. The Migration wizard creates a custom installation package and a remote installation task for it. The task scope will include the administration group that you selected on the **Managed devices to export** page; the task startup schedule will be set to **Manually** by default. The Migration wizard displays the creation progress. Wait until the refresh icons (↻) are replaced with the green check marks (✓) and click **Next**.

3. If necessary, select the **Run newly created remote installation task** check box (cleared by default) for the devices in the selected administration group of the Administration Server running on-premises and all of its subgroups. In this case, the devices will be switched under management of Kaspersky Next Expert View—but only after Network Agent installation completes. The full path will be displayed to the administration group in which the task will be run.

   The task must only be started after the import to Kaspersky Next Expert View finishes. Otherwise, the device names may be duplicated in the list.

4. Click **Finish** to close the Migration wizard and start the remote installation task for the following purposes:

   - Upgrading the Network Agent instances

   - Switching the Network Agent instances under management through Kaspersky Next Expert View

   If you have left the **Run newly created remote installation task** check box cleared, you can start the task later manually, if necessary.

You can check that you can now manage the migrated Network Agent instances through Kaspersky Next Expert View. To do this, go to **Asset management** → **Assets (Devices)**. Make sure that migrated managed devices have

the confirmation icon (⊘) in the **Visible**, **Network Agent is installed**, and **Network Agent is running** columns. Also, make sure that these devices do not have the *Not connected for a long time* status description.

Migration with a hierarchy of Administration Servers

This section describes the migration of managed devices and related objects from Kaspersky Security Center Web Console running on-premises to Kaspersky Next Expert View. The process involves a hierarchy: Kaspersky Security Center Web Console running on-premises acts as the secondary Administration Server and Kaspersky Next Expert View acts as the primary Administration Server.

Every administration group that you transfer to Kaspersky Next Expert View must contain the managed devices of a single operating system. If your network includes the devices of different operating systems, allocate them in different administration groups, and then migrate each group separately.

After you finish the migration, all Network Agents in the group within the migration scope are upgraded and managed through Kaspersky Next Expert View.

Before you start, do the following:

- Upgrade Administration Server running on-premises to version 14.2 or later.
- Install Kaspersky Security Center Web Console version 12.1 or later.
- Upgrade Network Agent on managed devices to version 12 or later.
- On Windows devices, use Network Agent without an uninstallation password.

  If the password has already been set, do one of the following in Kaspersky Security Center Web Console:

  - Disable the **Use uninstallation password** option in the Network Agent policy settings.
  - Uninstall Network Agent remotely by using the *Uninstall application remotely* task. In the **Application to uninstall** field of the task, select **Kaspersky Security Center Network Agent**. Do not forget to enter the uninstallation password.
- Upgrade the managed applications to the versions supported by Kaspersky Next Expert View.
- Make sure that you have policies for the latest versions of the managed applications. If you use outdated policies, create new ones for the application versions supported by Kaspersky Next Expert View.
- To use actual policies, upgrade the web plug-ins for the applications that you intend to manage through Kaspersky Next Expert View.
- Uninstall Kaspersky applications from managed devices if these applications are not supported by Kaspersky Next Expert View.

- Decrypt all the data (disk-level or file-level) that was encrypted by Kaspersky Endpoint Security for Windows on managed devices running the Windows operating system, and disable the encryption feature on the managed devices through the application policy or locally. For more information, see Help for Kaspersky Endpoint Security for Windows.

  If the Windows device still stores any files or folders encrypted through Kaspersky Endpoint Security for Windows, the Network Agent upgrade will be canceled during the migration process. A notification will prompt you to decrypt all data on the device and disable the encryption feature.

Kaspersky Next Expert View allows for a maximum of 25,000 managed devices per one Administration Server.

To perform a migration to Kaspersky Next Expert View:

1. Estimate the scope of the migration process, that is, review the administration group to export and assess the number of managed devices in it. Make sure that all the activities listed as migration prerequisites have been completed successfully.

2. In Kaspersky Next Expert View, proceed to the secondary Administration Server for the managed devices that you want to migrate.

3. In the main menu, go to **Operations** → **Migration**.

   The welcome page of the Migration wizard opens.

4. On the welcome page, click **Next**.

   The **Managed devices to export** page opens, displaying the entire hierarchy of administration groups of the secondary Administration Server.

5. On the **Managed devices to export** page, click the chevron icon (>) next to the **Managed devices** group name, and then expand the hierarchy of administration groups. Select the administration group that you want to export.

   The Migration wizard checks the total number of managed devices included in the selected administration group. If this number exceeds 10,000, an error message appears. The **Next** button remains unavailable (dimmed) until the number of managed devices in the selected administration group falls within the limit.

6. Select the managed applications whose policies and tasks must be transferred to Kaspersky Next Expert View together with group objects. To select the managed applications whose objects are to be exported, select the check boxes next to their names in the list.

   Although Kaspersky Security Center Administration Server is present on the list, selecting the corresponding check box does not result in the export of its policies.

   To make sure that your managed applications are supported by Kaspersky Next Expert View, click the corresponding link. It will redirect you to the Help article containing the list of applications managed by Kaspersky Next Expert View.

   If you select applications that are not supported by Kaspersky Next Expert View, the policies and tasks of these applications will be migrated anyway, but you will not be able to manage them in Kaspersky Next Expert View, due to the unavailability of the dedicated plug-ins.

7. View the list of group objects exported by default. You can also specify non-group objects to be exported together with the selected administration group, if necessary, such as global tasks, custom device selections, reports, custom roles, internal users and security groups, and custom application categories with content added manually. This page includes the following sections:

   - **Global tasks**

     The list of global tasks of managed applications, as well as global tasks of Network Agent.

     > If a global task that you selected applies to a specific object selection, this selection will also be exported.

     > Although the global tasks of Administration Server are present on the list, you cannot export them; selecting those tasks does not affect the export scope. Remote installation tasks also remain outside the export scope, because their respective installation packages cannot be exported.

   - **Device selections**

     The list of custom device selections.

   - **Reports**

     The editable list of report instances to be exported.

     > If a report that you selected applies to a specific object selection, this selection will also be exported.

     > Kaspersky Next Expert View contains the same set of report templates as Kaspersky Security Center Web Console, so you can select for export only the reports that you created manually or reconfigured.

   - **Group objects**

     The list of group objects to be exported by default. The following objects related to the selected administration group will be exported in their entirety by default:

     - Administration group structure, that is, all subgroups of the selected administration group.
     - Devices that have been included in the administration groups to be exported.
     - Tags that have been assigned to the devices to be exported.

       > If a tag was created in Kaspersky Security Center Web Console but never assigned to any device, it will not be exported. The auto-tagging rules will not be exported, either.

     - Group policies of the managed applications that have been selected.

       > Administration Server policies and Network Agent policies are not exported.

- Group tasks of the managed applications that have been selected and Network Agent group tasks.

  Administration Server tasks are not exported.

You can also prevent certain types of non-group objects from being exported:

- To cancel export for custom roles (that is, those created by the user only), select the **Exclude custom roles from export** check box.
- To cancel export for internal users and security groups, select the **Exclude internal users and security groups from export** check box.
- To cancel export for custom application categories with content added manually, select the **Exclude custom application categories from export** check box.

If you transfer devices of various operating systems to Kaspersky Next Expert View, non-group objects only need to be migrated once.

8. After you defined the migration scope, click **Next** to start the export process. The **Creating the export file** page opens, where you can view the export progress for each type of object that you included in the migration scope. Wait until each refresh icon (↻), located next to each item in the list of objects, is replaced with a green check mark (✓). The export finishes and the export file is automatically saved to a temporary folder. The next page opens, displaying the entire hierarchy of administration groups in Kaspersky Next Expert View, which acts as the primary Administration Server.

9. Select the check box next to the administration group to which the group objects must be imported, and then click **Next**. The file is unpacked, and the non-group objects and the group objects are restored to the target administration group.

   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.

   When the import completes, the exported structure of administration groups, including device details, appears under the target administration group that you selected. The non-group objects are also imported.

   You cannot minimize the Migration wizard and perform any concurrent operations during the import. Wait until each refresh icon (↻), located next to each item in the list of objects, is replaced with a green check mark (✓) and the import finishes. After this, the devices start switching to Kaspersky Next Expert View.

10. After the import completes, the Migration wizard displays a list of Network Agent installation packages available in Kaspersky Next Expert View for an appropriate operating system. Select the installation package containing the relevant version and localization of Network Agent.

    Select the Kaspersky Network Agent for Windows installation package only if you have previously completed the quick start wizard in your Kaspersky Next Expert View workspace and if you perform the migration of Windows devices.

11. Click **Next**.

    The Migration wizard creates a new stand-alone installation package (or uses an existing one) and a custom installation package based on it, as well as the corresponding remote installation task. The task scope includes the administration group that you selected on the **Managed devices to export** page. The task startup schedule is set to **Manually** by default. The Migration wizard displays the creation progress.

12. Wait until each refresh icon (↻) is replaced with a green check mark (✓), and then click **Next**.

13. If necessary, select the **Run newly created remote installation task** check box (cleared by default) for the devices in the selected administration group in Kaspersky Security Center Web Console running on-premises and all of its subgroups. After the Network Agent installation completes, you can manage the selected devices through Kaspersky Next Expert View. The full path is displayed to the administration group in which the task is to be run.

    The remote installation task must only be started after the import to Kaspersky Next Expert View finishes. Otherwise, the devices may be duplicated.

14. Click **Finish** to close the Migration wizard and start the remote installation task for the following purposes:

    - Upgrading the Network Agent instances
    - Managing the Network Agent instances through Kaspersky Next Expert View

    If you have left the **Run remote installation task** check box cleared, you can start the task later manually, if necessary.

You can check that you can now manage the migrated Network Agent instances through Kaspersky Next Expert View. To do this, go to **Asset management** → **Assets (Devices)**. Make sure that migrated managed devices have the confirmation icon (⊙) in the **Visible**, **Network Agent is installed**, and **Network Agent is running** columns. Also, make sure that these devices do not have the *Not connected for a long time* status description.

Scenario: Migration of devices running Linux or macOS operating systems

This section describes how to migrate devices running Linux or macOS operating systems from Kaspersky Security Center Web Console running on-premises to Kaspersky Next Expert View. The basic scenarios of migration without a hierarchy of Administration Servers and migration with such a hierarchy allow transferring all devices and related objects to Kaspersky Next Expert View. However, if your network includes devices running not only Windows, but also Linux or macOS, you need to transfer the devices of each operating system type separately. As a result, you have to perform the migration several times.

Prerequisites

Before you start, do the following:

- Upgrade Administration Server running on-premises to version 12 Patch A or later.
- Install Kaspersky Security Center Web Console version 12.1 or later.
- Upgrade Network Agent on managed devices to version 12 or later.
- Upgrade the managed applications to the versions supported by Kaspersky Next Expert View.
- Make sure that you have policies for the latest versions of the managed applications. If you use outdated policies, create new ones for the application versions supported by Kaspersky Next Expert View.
- To use actual policies, upgrade the web plug-ins for the applications that you intend to manage through Kaspersky Next Expert View.
- Uninstall Kaspersky applications from managed devices if these applications are not supported by Kaspersky Next Expert View, and then replace the uninstalled applications with supported ones.

Kaspersky Next Expert View allows for a maximum of 25,000 managed devices per one Administration Server.

Migration stages

Migration to Kaspersky Next Expert View comprises the following stages:

1. **Grouping managed devices by their operating systems**

   If your network includes devices running different operating systems (Windows, Linux, or macOS), place the devices of each operating system in separate administration groups in Kaspersky Security Center Web Console. Also, create an administration group for each Linux distribution. For example, if you have Debian and Red Hat Linux devices, allocate them in different administration groups. This will allow you to perform the migration successfully because different Network Agent installation packages are required for various operating systems.

2. **Perform separately the migration of every administration group and its application objects**

   The managed devices of each operating system must migrate separately, to include their policies and tasks. For example, if you have Windows, macOS, Ubuntu, and CentOS devices, first, transfer the devices running the Windows operating system to Kaspersky Next Expert View, then macOS, then Ubuntu, and eventually, CentOS. You can transfer the managed devices in any order.

   To do this, perform the migration without the hierarchy of Administration Servers or migration with such a hierarchy, depending on whether your network includes secondary Administration Servers. During the migration, use the Network Agent installation package corresponding to the operating system of the transferred devices. For example, select the Kaspersky Security Center 13.2 Network Agent for Linux devices to perform the migration successfully.

Note that non-group objects, such as global tasks, custom device selections, or reports, only need to be migrated once.

Results

Upon finishing with the migration, you can make sure that it was successful:

- The proper version of Network Agent is re-installed on each managed device running the Linux or macOS operating system.
- All Linux or macOS devices are managed through Kaspersky Next Expert View.
- All object settings that were effective before migration are preserved.

Scenario: Reverse migration from Kaspersky Next Expert View to Kaspersky Security Center

You may want to migrate the managed devices from Kaspersky Next Expert View to Kaspersky Security Center Administration Server. For example, this process can be used to roll back migration to Kaspersky Next Expert View.

Prerequisites

Make sure that the following prerequisites are met:

- Kaspersky Next Expert View is available and has managed devices connected.
- Kaspersky Security Center 14.2 (or later) Administration Server is available and has a Network Agent installation package of version 13 or later.

Reverse migration stages

Reverse migration comprises the following stages:

1. **Creating a Network Agent stand-alone installation package in Kaspersky Security Center Administration Server on-premises**

   In Kaspersky Security Center Administration Server running on-premises, create a Network Agent stand-alone installation package.

During the creation process, you can select the **Move unassigned devices to this group** option to specify an administration group to which you want to move Network Agents after installation. If you have specified the administration group, an automatic moving rule is created that will move to the target administration group all Network Agents installed with this stand-alone installation package.

To ensure correct reverse migration, make sure that you select the Network Agent version that is equal to or later than the version used in Kaspersky Next Expert View.

2. **Creating a custom installation package in Kaspersky Next Expert View**

   In Kaspersky Next Expert View, create a custom installation package based on the stand-alone installation package that you created and saved from Kaspersky Security Center Administration Server running on-premises.

   To enable package installation in silent mode, in the **Executable file command line** field, specify the `-s` key.

3. **Creating a remote installation task**

   In Kaspersky Next Expert View, create a remote installation task using the custom installation package that you have created.

4. **Running the remote installation task**

   Start the remote installation task that you created. The task initiates the re-installation of all Network Agents in the specified administration group; and it also switches the Network Agents under management of Kaspersky Security Center Administration Server running on-premises by changing the connection address and modifying other connection settings.

   If you did not specify any target administration group during creation of the stand-alone installation package, all devices are moved to the **Unassigned devices** group.

Results

Upon finishing with the migration, you can make sure that it was successful:

- All devices within the scope of the remote installation task that were previously managed through Kaspersky Next Expert View are now managed by Kaspersky Security Center Administration Server running on-premises.
- The devices are automatically moved to the administration group specified in the installation package settings.

The remote installation task in Kaspersky Next Expert View cannot be completed: it has no more target devices since all of them have modified connection settings. You have to stop the task manually after you make sure that the error icon (!) has appeared in the **Visible** column of the Managed Devices list for all devices from the migration scope.

Migration with virtual Administration Servers

If you have virtual Administration Servers in your existing Kaspersky Security Center on-premises infrastructure, you cannot migrate from Kaspersky Security Center on-premises to Kaspersky Next Expert View by using the Migration wizard. Also, you will be able to migrate only your customers' devices. You will have to create policies, tasks, and reports manually.

You can perform one of the following migration scenarios:

- By moving your client devices from virtual Administration Servers to a primary Administration Server
- By performing manual migration from virtual Administration Servers

Scenario: Migration with virtual Administration Servers by moving devices

To perform the migration from Kaspersky Security Center Web Console running on-premises to Kaspersky Next Expert View, you can move your devices from virtual Administration Servers to a primary Administration Server.

Prerequisites

Before migration, you must perform a number of actions, including upgrading Administration Server running on-premises to version 12 or later and upgrading the managed applications to versions supported by Kaspersky Next Expert View.

Migration scenario

The scenario proceeds in stages:

1. **Creating an administration group for each of your virtual Administration Servers**

   You create the group in your Kaspersky Security Center running on-premises.

2. **Moving your customers' devices**

   In Kaspersky Security Center running on-premises, move your customers' devices from each virtual Administration Server to the respective administration group created at the previous stage.

3. **Migration**

   Perform migration as described for the network without a hierarchy of Administration Servers.

4. **Moving devices under management of virtual Administration Servers (optional step)**

   If you want to manage your customers through virtual Administration Servers, move the devices from the administration groups under management of virtual Administration Servers.

5. **Creating policies, tasks, and reports**

   Create policies, tasks, and reports as required.

Results

Upon finishing with the migration, you can make sure that it was successful:

- Network Agent is re-installed on all managed devices.
- All devices are managed through Kaspersky Next Expert View.
- All object settings that were effective before migration are preserved.

Scenario: Manual migration with virtual Administration Servers

You can migrate from Kaspersky Security Center Web Console running on-premises to Kaspersky Next Expert View manually.

Prerequisites

Before migration, you must perform a number of actions, including upgrading Administration Server running on-premises to version 12 or later and upgrading the managed applications to versions supported by Kaspersky Next Expert View.

Migration scenario

The scenario proceeds in stages:

1. **Creating an administration group for each of your virtual Administration Servers**

   In Kaspersky Next Expert View, create an administration group that corresponds to each of your virtual Administration Servers.

2. **Creating a stand-alone installation package for Network Agent**

   Create a stand-alone installation package for Network Agent. During creation, specify the administration group that you created at the previous stage. This means that you must create an individual stand-alone installation package for each administration group.

   This stage occurs in your Kaspersky Next Expert View.

3. **Downloading the stand-alone installation packages**

   Download the stand-alone installation packages that you created at the previous stage. This stage occurs in your Kaspersky Next Expert View.

4. **Creating an archive with each stand-alone installation package**

   Available archive types are: ZIP, CAB, TAR, or TAR.GZ.

5. **Creating custom installation packages for Network Agent**

   Create custom installation packages for Network Agent. During creation, use archives that you created at the previous stage.

   This stage occurs in your Kaspersky Security Center running on-premises.

6. **Creating remote installation tasks**

   Create remote installation tasks to install Network Agent from the created custom installation packages.

   When creating a task, specify a corresponding administration group.

   This stage occurs in your Kaspersky Security Center running on-premises.

7. **Running the created remote installation tasks**

   Network Agents are updated. The Kaspersky Next Expert View Administration Server takes over the management of them.

   All devices are migrated to Kaspersky Next Expert View and are placed in administration groups that were specified when you created stand-alone installation packages for Network Agent.

8. **Moving devices under management of virtual Administration Servers (optional step)**

   If you want to manage your customers through virtual Administration Servers, move the devices from the administration groups under management of virtual Administration Servers.

9. **Creating policies, tasks, and reports**

   Create policies, tasks, and reports as required.

Results

Upon finishing with the migration, you can make sure that it was successful:

- Network Agent is re-installed on all managed devices.
- All devices are managed through Kaspersky Next Expert View.

  All object settings that were effective before migration are preserved.

Scenario: Moving devices from administration groups under management of virtual Servers

You may want to manage your customers through virtual Administration Servers. If you migrated devices and other items from Kaspersky Security Center on-premises to Kaspersky Next Expert View, the devices are located in administration groups. To manage the customers' devices through virtual Administration Servers, you must move the devices from the administration groups under the management of virtual Administration Servers.

Prerequisites

You have created a virtual Administration Server for each of your customers.

All devices of each customer are located in an individual administration group.

Stages

The scenario proceeds in stages:

1. **Creating a stand-alone installation package for Network Agent**

   Switch to each of the created virtual Administration Server, then create a stand-alone installation package for Network Agent. You can switch Administration Servers in the main menu by clicking the chevron icon (›) to the right of the current Administration Server name, and then selecting the required Administration Server.

2. **Downloading the stand-alone installation packages**

   Download the stand-alone installation packages that you created at the previous stage.

3. **Creating an archive with each stand-alone installation package**

   Available archive types are: ZIP, CAB, TAR, or TAR.GZ.

4. **Creating custom installation packages for Network Agent**

   Create custom installation packages for Network Agent. During creation, use archives that you created at the previous stage.

   This stage occurs on the primary Administration Server.

5. **Creating remote installation tasks**

   Create remote installation tasks to install Network Agent from the created custom installation packages.

   When creating a task, specify a corresponding administration group.

   This stage occurs on the primary Administration Server.

6. **Running the created remote installation tasks**

   Network Agents are updated. The devices are moved under management of virtual Administration Servers.

7. **Creating policies, tasks, and reports**

   Create policies, tasks, and reports as required.

Results

You can now manage the migrated customers' devices by using virtual Administration Servers.

Quick start wizard

This section provides information about the Kaspersky Next Expert View quick start wizard.

About quick start wizard

The quick start wizard in Kaspersky Next Expert View enables you to create a minimum of necessary tasks and policies, adjust a minimum of settings, and start creating installation packages of Kaspersky applications. Using the wizard, you can make the following changes to Kaspersky Next Expert View:

- Initiate downloading of installation packages for managed Kaspersky applications.
- Create a Network Agent stand-alone installation package for devices running Windows, Linux, or macOS.
- Create Kaspersky Security Center Network Agent policy.
- Create the *Download updates to the repositories of distribution points* task
- Create policies and tasks for managed Kaspersky applications.
- Configure interaction with Kaspersky Security Network (KSN).

After the quick start wizard has finished, installation packages for Network Agent and managed Kaspersky applications appear in the **Discovery & deployment** → **Deployment & assignment** → **Installation packages** list.

The quick start wizard creates policies for managed applications, such as Kaspersky Endpoint Security for Windows, unless such policies are created for the Managed devices group. The quick start wizard creates tasks if tasks with the same names do not exist for the Managed devices group.

Kaspersky Next Expert View automatically prompts you to run the quick start wizard after you have created a company workspace and have started Kaspersky Next Expert View for the first time. You can also start the quick start wizard manually at any time.

Starting quick start wizard

Kaspersky Next Expert View automatically prompts you to run the quick start wizard after you have created a company workspace and have started Kaspersky Next Expert View for the first time. You can also start the quick start wizard manually at any time.

If you start the quick start wizard again, tasks and policies created at the previous run of the wizard are not created again.

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.

3. Click **Start quick start wizard**.

   Alternatively, you can start the quick start wizard by selecting **Discovery & deployment** → **Deployment & assignment** → **Quick start wizard**.

The wizard prompts you to perform initial configuration of Kaspersky Next Expert View. Follow the steps of the wizard. Proceed through the wizard by using the **Next** button. Use the **Back** button to return to the previous step of the wizard.

Step 1. Selecting installation packages to download

In the list, select the Kaspersky applications to install on the client devices. Kaspersky Next Expert View will create installation packages for the selected applications. Afterwards, you will use the created installation packages to install the applications.

When selecting an installation package to download, pay attention to the language: installation packages are available in different languages.

Select the following applications:

- Kaspersky Security Center Network Agent

  When selecting Network Agent installation packages, consider the following:

  - Network Agent must be installed on every client device. Therefore, select a Network Agent appropriate for each operating system running on the client devices.

  - Network Agent must be installed manually through a stand-alone installation package on a device that you select to act as a distribution point. Distribution points are required to perform network polling and remote installation of Kaspersky security applications on client devices. Therefore, you must select at least one installation package of Network Agent. While you proceed to the next steps of the wizard, Kaspersky Next Expert View creates the Network Agent stand-alone installation package.

    Compared to Windows-based distribution points, Linux-based and macOS-based distribution points have limited functionality. It is strongly recommended that you select Windows-based computers to act as distribution points.

    You can select Network Agents for Windows, Linux, and macOS. If you select Network Agent only for one operating system, for example, macOS, then a stand-alone installation package will be created for the selected operating system. If you select Network Agent for several operating systems, Kaspersky Next Expert View creates only one stand-alone installation package according to the following priorities: Windows is of the highest priority, then Linux, and then macOS. For example, if you select Network Agents for Linux and macOS, then Kaspersky Next Expert View creates a stand-alone installation package for Network Agent for Linux. You can create a Network Agent stand-alone installation package for any of these operating systems manually at any time.

- Kaspersky security applications

  Select installation packages appropriate for the operating systems that are installed on client devices in your organization.

Step 2. Configuring a proxy server

If your organization uses a proxy server to connect to the internet, specify the proxy server settings at this step of the wizard. These settings are added to the Network Agent installation package. After installation, Network Agent automatically uses these settings on each client device.

Specify the following settings for a proxy server connection:

- **Use proxy server**
- **Address**
- **Port number**
- **Proxy server authentication**

  If this option is enabled, in the entry fields you can specify the credentials for proxy server authentication.

  We recommend that you specify the credentials of an account that has minimum privileges required only for the proxy server authentication.

  By default, this option is disabled.

- **User name**

  User name 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.

- **Password**

  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.

Step 3. Configuring Kaspersky Security Network

If at the first step of the wizard you downloaded the Kaspersky Endpoint Security for Windows installation package, the text of the KSN Statement for the following applications is displayed:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security Center installed on local devices
- Kaspersky Next Expert View installed in the cloud environment

If you did not download the Kaspersky Endpoint Security for Windows installation package, the KSN Statement for this application is not displayed.

In trial mode, only the KSN Statement for Kaspersky Endpoint Security for Windows is displayed.

Carefully read the Kaspersky Security Network Statement. Choose one of the following options:

- **I agree to participate in Kaspersky Security Network**

  Kaspersky Next Expert View 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 Next Expert View 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.

By default, the use of KSN is disabled. Later, if you change your mind about using KSN, you can enable (or disable) the corresponding option in the Administration Server properties window, in the **KSN Settings** section.

Step 4. Configuring third-party update management

This step is not displayed if the *Find vulnerabilities and required updates* task already exists.

If you want to get a list of updates for the applications installed on the managed devices and a list of found vulnerabilities and recommended fixes for them, enable the **Search for third-party software updates and vulnerability fixes** option. If this option is enabled, Kaspersky Next Expert View creates the *Find vulnerabilities and required updates* task.

Step 5. Creating a basic network protection configuration

At this step of the wizard, click the **Create** button to create objects required for initial protection of your client devices.

Kaspersky Next Expert View performs two operations:

- Creating basic policies and tasks with default settings

  The following policies are created:

  - Kaspersky Security Center Network Agent policy
  - Policies for managed Kaspersky applications

The following tasks are created:

- The *Download updates to the repositories of distribution points* task
- The *Find vulnerabilities and required updates* task

  This task is only created if you enabled the **Search for third-party software updates and vulnerability fixes** option on the previous step of the wizard.

- Tasks for managed Kaspersky applications

- Creating a stand-alone installation package for Network Agent

  You will use this package to install Network Agent on distribution points. Kaspersky Next Expert View creates the stand-alone installation package on the basis of the Network Agent installation package that you selected at the previous step of the wizard. During the package creation, you must read and accept the terms of EULA for Network Agent. When the stand-alone installation package is created, you will be prompted to download it to the device you are using at the moment.

  Network Agent stand-alone installation package creation can take some time. Go to the next step of the wizard. The process will continue in background mode. If necessary, you can track the installation package download status in the **Package status** column (**Discovery & deployment** → **Deployment & assignment** → **Installation packages**).

For authentication reasons, each stand-alone installation package is signed by using a certificate. The certificate is reissued every 3 months. After each procedure of certificate reissue, Kaspersky Next Expert View automatically updates the signatures of all created stand-alone installation packages. For downloaded stand-alone installation packages, an automatic signature update cannot be performed. Therefore, the certificate expires and a certificate error might occur while you install an application from a stand-alone installation package. In this case, download the stand-alone installation package again.

Also, you can view the certificate validity period in the properties of the stand-alone installation package file downloaded to your device. To do it, right-click the stand-alone installation package, and go to its details. On the **Digital Signatures** tab, you have to select the required certificate in the list, click the **Details** button, and then in the window that opens, click the **View Certificate** button.

Step 6. Closing the quick start wizard

On the quick start wizard completion page, read about the additional operations you must perform in order to deploy Kaspersky security applications on the client devices. Follow the stages provided in the scenario of Kaspersky applications initial deployment.

Kaspersky applications initial deployment

This section describes the initial deployment of Kaspersky applications on client devices in your organization.

Scenario: Kaspersky applications initial deployment

This scenario describes how to install Kaspersky applications on client devices in Kaspersky Next Expert View. First, you must deploy distribution points on your network. Then, by means of the distribution points, you must perform network polling and discover networked devices on your network. After that, you can deploy Kaspersky applications on networked devices.

When the scenario is complete, the Kaspersky applications are deployed on the selected client devices in your organization's network. You can manage all the devices with Kaspersky applications installed.

Prerequisites

Make sure that the following prerequisites are met:

- The quick start wizard has finished.
- Network Agent and security applications installation packages are created.
- You have information about internet settings for client devices in your organization, information about the gateway, and proxy server settings.
- Client devices in your organization are not encrypted.

Stages

The Kaspersky applications initial deployment proceeds in stages:

1. **Selecting a device to act as a distribution point**

   In Kaspersky Next Expert View, a distribution point is intended for:

   - Network polling and device discovery
   - Remote installation of Network Agent on client devices
   - Connection of client devices to Administration Server (when a distribution point is acting as a connection gateway)

   Select a device on your organization's network to act as a distribution point for an administration group. The selected device must meet the requirements for distribution point. Depending on the amount of client devices in your organization's network, select the correct number of devices to act as distribution points.

2. **Creating a stand-alone installation package for Network Agent**

   Create a stand-alone installation package for Network Agent to install on the distribution point.

   If your client devices do not have direct internet access to connect to Administration Server, in the Network Agent installation package settings, configure the connection gateway and proxy server settings.

3. **Installing Network Agent on the selected device to act as a distribution point**

   Deliver the stand-alone installation package for Network Agent to the selected device by any method. For example, you can copy the stand-alone installation package to a removable drive (such as a flash drive), or place it in a shared folder.

   In the **Properties** window of the stand-alone installation package file, verify that the stand-alone installation package for Network Agent is signed by Kaspersky.

   Run the installation of the stand-alone installation package for Network Agent on the selected device. Network Agent is now installed according to the settings of the Network Agent installation package and is connected to Administration Server. The device with Network Agent is placed in the administration group that was specified when the stand-alone installation package for Network Agent was created.

   If you install Network Agent by using a stand-alone installation package on a device running Microsoft Windows XP Professional for Embedded Systems 32-bit, the installation fails. To resolve this issue, preliminarily install the update KB2868626 for Windows XP from the Microsoft website: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

4. **Assigning the device with Network Agent installed to act as a distribution point**

   Assign the device with Network Agent installed to act as a distribution point.

5. **Configuring and performing network polling for the distribution point**

   Configure network polling for the distribution point with the Network Agent installed. As an option, you can configure network polling in the Network Agent policy.

   After network polling according to schedule is complete, the client devices connected to your organization's network are discovered and placed in the **Unassigned devices** group.

6. **Creating installation packages for Network Agent and managed Kaspersky applications**

   If you did not start the quick start wizard, or skipped the step of creating installation packages, create installation packages for Kaspersky applications. You must create installation packages both for Network Agent and for managed Kaspersky applications appropriate for the operating system installed on client devices on your organization's network.

7. **Removing third-party security applications**

   If third-party security applications are installed on client devices on your organization's network, remove them before installing the Kaspersky application.

8. **Installing Kaspersky applications on client devices**

   Create tasks to install Network Agent and managed Kaspersky applications on client devices on your organization's network. When creating the tasks, use the **Install application remotely** task type. For the task to install Network Agent, use the **Using operating system resources through distribution points** option. For the task to install managed Kaspersky applications, use the **Using Network Agent** option. After the tasks are created, you can configure their settings. Make sure that the schedule for each task meets your requirements. First, the task to install Network Agent must be run. Then, after Network Agent is installed on client devices, the task to install managed Kaspersky applications must be run.

As an option, you can create one remote installation task to install Network Agent and managed Kaspersky applications on client devices on your organization's network. In this case, in the **Installation packages** block, use the **Select installation package** option and the **Select Network Agent** option; in the **Force installation package download** block, use the **Using operating system resources through distribution points** option.

You also can create several remote installation tasks to install managed Kaspersky applications for different administration groups or different device selections.

If you have client devices that are out of the network with distribution point, for example, laptops of remote users, you must create and deliver the Network Agent stand-alone installation package to those client devices by any method. Install Network Agent stand-alone installation package locally on those client devices. Then you can install managed Kaspersky applications on those remote users' devices following the same instructions as for other devices discovered by the distribution point.

Run the remote installation tasks.

As an option, to install Kaspersky applications, you can start the Protection deployment wizard.

9. **Installing Kaspersky Security for Mobile**

   If you plan to manage corporate mobile devices, follow the instructions provided in the Kaspersky Security for Mobile Help for information about deployment of Kaspersky Endpoint Security for Android.

10. **Verifying initial deployment of Kaspersky applications**

    Generate and view the **Report on Kaspersky application versions**. Make sure that the managed Kaspersky applications are installed on all client devices in your organization.

For the full disk encryption, Kaspersky Next Expert View supports only BitLocker.

Creating installation packages for Kaspersky applications

To deploy Kaspersky applications on networked devices in your organization, you must create installation packages of Kaspersky applications in Kaspersky Next Expert View.

To create a Kaspersky application installation package:

1. Do one of the following:

   - In the main menu, go to **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.
   - In the main menu, go to **Operations** → **Repositories** → **Installation packages**.

   You can also view notifications about new packages 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.

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**.

   A list of distribution packages available on Kaspersky web servers appears. 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.

4. Click the name of a distribution package, for example, **Kaspersky Endpoint Security for Windows (<version number>)**.

   A window opens with information about the distribution package.

5. Read the information and click the **Download and create installation package** button.

   If the distribution package cannot be automatically converted into an installation package, **Download and create installation package** button is displayed instead of the **Download distribution package** button. In this case, download the distribution package, and then use the downloaded file to create a custom installation package.

   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** button to read License Agreements.

   b. In the opened pane, read License Agreements that are displayed on the screen.

      To view the data processed by Kaspersky applications for which you want to create an installation package, click **View the list of data**.

   c. Select License Agreements, and then click **Accept**.

   The download continues after you accept License Agreements. If you click **Decline**, the download is stopped.

   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 in the beginning of the list.

   If you plan to perform migration from Kaspersky Security Center Web Console to Kaspersky Next Expert View and your organization's security regulations require the use of proxy when accessing the corporate network, this may affect the migration process. After you create a Network Agent installation package, you must specify the proxy settings to ensure connection between the Network Agent instances on managed devices and your Kaspersky Next Expert View workspace:

   a. Click the installation package name.

   b. In the installation package properties window that opens, go to the **Settings** tab.

   c. Open the **Connection** section.

   d. Select the **Use proxy server** option and fill in the **Proxy server address** and **Proxy server port** fields.

6. When the download is complete, click the **Close** button () to close the window with information about the distribution package.

The installation package is created. The installation package appears in the list of installation packages.

You cannot add an installation package with the same localization language several times. For example, if you already added the Kaspersky Endpoint Security for Windows (English) installation package, you can add Kaspersky Endpoint Security for Windows installation packages localized in other languages, except English.

Distributing installation packages to secondary Administration Servers

To distribute installation packages to secondary Administration Servers:

1. Establish a connection with the Administration Server that controls the relevant secondary Administration Servers.

2. Create a task of installation package distribution to secondary Administration Servers in one of the following ways:

   - If you want to create a task for secondary Administration Servers in the selected administration group, launch the creation of a group task for this group.

   - If you want to create a task for specific secondary Administration Servers, launch the creation of a task for specific devices.

   The New task wizard starts. Follow the steps of the wizard.

   In the **New task** window of the New task wizard, in the **Task type** field select **Distribute installation package**. You can also edit the default name of the task in the **Task name** field.

   At the next step, specify the secondary Administration Servers for the task scope and follow the instructions of the New task wizard. When you finish, the New task wizard will create the task of distributing the selected installation packages to specific secondary Administration Servers.

   > When you create the Distribute installation package task for secondary Administration Servers running on-premises, the distribution scope—aside from custom installation packages—will only include the installation packages of Kaspersky applications that are supported by Kaspersky Security Center Web Console running on-premises, regardless of which distribution option has been selected (**All installation packages** or **Selected installation packages**).

3. Run the task manually or wait for it to launch according to the schedule that you specified in the task settings.

The selected installation packages will be copied to the specific secondary Administration Servers.

Creating a stand-alone installation packages for Network Agent

You and device users in your organization can use stand-alone installation packages to install Network Agent on devices locally. Stand-alone installation packages can be created for devices running Windows, Linux, or macOS.

> In Kaspersky Next Expert View, you can create stand-alone installation packages only for Network Agent.

A stand-alone installation package is an executable file that can be 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 Network Agent without involving Kaspersky Next Expert View.

For Network Agent for Linux and Network Agent for macOS, the stand-alone installation package is a script file with the .sh extension. When you run this file, the script unpacks the attached archive, which contains the installation package and its settings, and then starts the installation.

If the Administration Server has access to Internet, the **Download updates to the Administration Server repository** task is used to download dependencies required for creating Network Agent stand-alone installation packages. If the Administration Server does not have access to Internet, perform the following steps:

1. Execute the following command to create the RIUtilsArchiveDirUsed flag:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Execute the following command to restart the Administration Server service:

   ```
   systemctl restart kladminserver_srv.service
   ```

Download the following archives from the Kaspersky website and place the archives in the /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives folder:

- ri_utils_win32.zip
- ri_utils_arm64.zip

Do not rename the archives.

The Administration Server now has the required dependencies.

If you install Network Agent by using a stand-alone installation package on a device running Microsoft Windows XP Professional for Embedded Systems 32-bit, the installation fails. To resolve this issue, preliminarily install the update KB2868626 for Windows XP from the Microsoft website: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

For authentication reasons, each stand-alone installation package is signed by using a certificate. The certificate is reissued every 3 months. After each procedure of certificate reissue, Kaspersky Next Expert View automatically updates the signatures of all created stand-alone installation packages. For downloaded stand-alone installation packages, an automatic signature update cannot be performed. Therefore, the certificate expires and a certificate error might occur while you install an application from a stand-alone installation package. In this case, download the stand-alone installation package again.

Also, you can view the certificate validity period in the properties of the stand-alone installation package file downloaded to your device. To do it, right-click the stand-alone installation package, and go to its details. On the **Digital Signatures** tab, you have to select the required certificate in the list, click the **Details** button, and then in the window that opens, click the **View Certificate** button.

To create a stand-alone installation package:

1. Do one of the following:

   - In the main menu, go to **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.
   - In the main menu, go to **Operations** → **Repositories** → **Installation packages**.

   A list of installation packages is displayed. If the Network Agent installation package is not in the list, create this installation package manually.

2. In the list of installation packages, click the name of the Network Agent installation package.

   The properties window of the Network Agent installation package opens.

3. Configure settings of the Network Agent installation package, if necessary, and close the properties window of the Network Agent installation package.

4. In the list of installation packages, select an installation package and, above the list, click the **Deploy** button.

5. 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.

6. 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.

7. 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, do not change choice of option.

   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.

8. Select the **Open the list of stand-alone packages** option if you want the list of stand-alone installation packages to be displayed after the wizard is finished.

9. Click the **Finish** button.

   The Stand-alone Installation Package Creation Wizard closes.

The Network Agent stand-alone installation package is created. The created stand-alone installation package is displayed in the list of stand-alone installation packages, which you can view.

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:

1. In the main menu, go to **Operations** → **Installation packages**.

   A list of installation packages is displayed.

2. Above the list, click the **View the list of stand-alone packages** button.

A list of stand-alone installation packages is displayed.

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.
- **Network Agent installation package name**.
- **Network Agent version**.
- **Size**. File size in megabytes (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.
- **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 that you created and transferred to the user.

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:

- Remove a stand-alone installation package by clicking the **Remove** button.
- Download a stand-alone installation package to your device by clicking the **Download** button.

  For authentication reasons, each stand-alone installation package is signed by using a certificate. The certificate is reissued every 3 months. After each procedure of certificate reissue, Kaspersky Next Expert View automatically updates the signatures of all created stand-alone installation packages. For downloaded stand-alone installation packages, an automatic signature update cannot be performed. Therefore, the certificate expires and a certificate error might occur while you install an application from a stand-alone installation package. In this case, download the stand-alone installation package again.

Also, you can view the certificate validity period in the properties of the downloaded stand-alone installation package. To do it, on the **Digital Signatures** tab, you have to select the required certificate in the list, click the **Details** button, and then in the window that opens, click the **View Certificate** button.

Creating custom installation packages

You can use custom installation packages to do the following:

- To install any application (for example, a text editor) on a client device involving Kaspersky Next Expert View, 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, including an executable file. A 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. Creating a custom installation package, you can specify command-line options, for example, to install the application in a silent mode.

> You cannot create custom installation packages in the trial mode of Kaspersky Next Expert View.

To create a custom installation package:

1. Do one of the following:
   - In the main menu, go to **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.
   - In the main menu, go to **Operations** → **Repositories** → **Installation packages**.

   A list of installation packages available on 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 from a file**.
4. Specify the package name and click the **Browse** button.

   A standard **Open** window lets you choose an archive file to create the installation package.
5. Select 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.

   Files are downloaded to the Kaspersky Next Expert View Administration Server.

   If Administration Server detects that the archive includes Kaspersky application, an error message is displayed. You can download installation packages for Kaspersky applications from Kaspersky Web Servers. This operation is available by selecting **Operations** → **Kaspersky applications** → **Current application versions**.
6. If the selected archive file includes several executable files, select one executable file that has to be run to install the application using the created installation package.
7. If you want, specify an executable file command-line parameters.

You can specify command-line parameters to install the application from the installation package in a silent mode. Refer to the application vendor's documentation for details of the command-line parameters.

Creation of the installation package starts.

The wizard informs you when the process is finished.

If the installation package is not created, an error message is displayed.

In Kaspersky Next Expert View, the total size of all custom installation packages on the Administration Server is limited to 500 MB. If this limit is exceeded while creating a new custom installation package, delete older custom installation packages created earlier. The size of an installation package is displayed in its properties.

8. Click the **Finish** button to close the wizard.

The created custom installation package is downloaded to the Administration Server. After downloading, the installation package appears in the list of installation packages.

In the list of installation packages, you can view the following properties of a custom 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 custom installation package.
- **OS**. Operating system for which the custom installation package is created.
- **Created**. Installation package creation date.
- **Modified**. Installation package modification date.
- **Type**. Kaspersky application or third-party application.

In the list of installation packages, by clicking the link with the name of a custom installation package, you can change command-line parameters and the custom installation package name.

Requirements for a distribution point

To handle up to 10,000 client devices, a distribution point must meet, at a minimum, the following requirements (a configuration for a test stand is provided):

- CPU: Intel® Core™ i7-7700 CPU, 3.60 GHz 4 cores.
- RAM: 8 GB
- Free storage space: 120 GB.

In addition, a distribution point must have internet access and must always be connected.

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.

Network Agent installation package settings

To configure a Network Agent installation package:

1. Do one of the following:

   - In the main menu, go to **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.
   - In the main menu, go to **Operations** → **Repositories** → **Installation packages**.

   A list of installation packages available on Administration Server is displayed.

2. Click the link with the name of the Network Agent installation package.

   The properties window of the Network Agent installation package opens. The information in the window is grouped on tabs and in sections.

General

The **General** section displays general information about the installation package:

- Installation package language
- 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

This section presents the settings required to ensure proper functioning of Network Agent immediately after it is installed. The settings in this section are available only on devices running Windows.

In the **Destination folder** group of settings, you can select the client device folder in which Network Agent will be installed.

- **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.

In the following group of settings, you can set a password for the Network Agent remote uninstallation task:

- **Use uninstallation password**

  If this option is enabled, by clicking the **Modify** button you can enter the uninstall password (only available for Network Agent on devices running Windows operating systems).

  By default, this option is disabled.

- **Status**

- **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.

- **Automatically install applicable updates and patches for components that have the Undefined status**

  If this check box is selected, all downloaded updates and patches for Network Agent will be installed automatically.

  If this check box is cleared, 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 check box is enabled.

Connection

In this section, you can configure connection of Network Agent to the Administration Server:

- **Use UDP port**

  UDP port number

  In this field you can specify the port to connect Administration Server to Network Agent using UDP protocol.

  The default UDP port is 15000.

- **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.

- **Do not use proxy server**

- **Use proxy server**

  If this option is enabled, an internet proxy server is used to connect the Network Agent to the Administration Server and a connection gateway.

  Proxy server address

  Proxy server port

- **Proxy server authentication**

  If this option is enabled, in the entry fields you can specify the credentials for proxy server authentication.

  We recommend that you specify the credentials of an account that has minimum privileges required only for the proxy server authentication.

  By default, this option is disabled.

  User name

  User name 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.

  Password

  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.

For compatibility purposes, it is not recommended to specify proxy connection settings in the Network Agent installation package settings.

Advanced

In this section, you can configure how the connection gateway and virtual machine are used, as well as whether to register a user as a device owner:

- **Connect to Administration Server by using a connection gateway**

  Only a direct connection to connection gateways is supported. The option of using an internet proxy server specified in the installation package will not be applied.

- **Connection gateway address**

- **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 VDI**

  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.

- **Allow running the user registration utility after Network Agent installation**

  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.

Additional components

In this section you can select additional components for concurrent installation with Network Agent.

Tags

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.

Revision history

In this section, 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.

Network Agent installation package settings available to a specific operating system are given in the table below.

Network Agent installation package settings

Property section	Windows	Mac	Linux
General	✓	✓	✓
Settings	✓	—	—

Property section	Windows	Mac	Linux
Connection	✓	✓ * except the **Open Network Agent ports in Microsoft Windows Firewall** check box	✓ * except the **Open Network Agent ports in Microsoft Windows Firewall** check box
Advanced	✓	✓	✓
Additional components	✓	✓	✓
Tags	✓	✓ * except the automatic tagging rules	✓ * except the automatic tagging rules
Revision history	✓	✓	✓

Virtual infrastructure

Kaspersky Next Expert View supports the use of virtual machines. To protect your virtual infrastructure, you need to install Network Agent on each virtual machine.

Tips on reducing the load on virtual machines

When installing Network Agent on a virtual machine, you are advised to consider disabling some Kaspersky Next Expert View 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 Administration Console.

Support of dynamic virtual machines

Kaspersky Next Expert View 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. The virtual machine with installed Network Agent is also added to the Administration Server database. After you turn off this 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

Kaspersky Next Expert View supports copying a virtual machine with installed Network Agent or creating one from a template with installed Network Agent.

Network Agent can automatically detect copying of virtual machines in the following cases:

- 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.

Usage of Network Agent for Windows, Linux, and macOS: Comparison

Network Agent for macOS and Linux has several functional limitations compared to Network Agent for Windows. 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, macOS, and Linux operating systems.

Network Agent feature comparison

Network Agent feature	Windows	Linux	macOS
Installation			
Automatic installation of updates and patches for Network Agent	✓	✓	–
Automatic distributing of a key	✓	✓	✓
Installing manually, by running application installers on devices	✓	✓	✓
Forced synchronization	✓	✓	✓ Except a push server
Distribution point			
Network polling	✓ • IP range polling • Windows network polling • Domain controller polling (Microsoft Active Directory)	✓ • IP range polling • Domain controller polling (Microsoft Active Directory, Samba as an Active Directory, FreeIPA, ALD Pro)	–
Running KSN proxy service on a distribution point side	✓	✓	–
Downloading updates via Kaspersky update servers to the distribution points repositories that distribute updates to managed devices	✓	✓	– Distribution point devices running macOS cannot download updates from Kaspersky update servers. If one or more devices running 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	✓	Restricted: it is not possible to perform push installation on Windows devices by using Linux distribution points.	Restricted: it is not possible to perform push installation on Windows devices by using macOS distribution points.
Handling third-party applications			
Remote installing of applications on devices	✓	–	–
Software updates	✓	–	–
Configuring operating system updates in a Network Agent policy	✓	–	–

Network Agent feature	Windows	Linux	macOS
Viewing information about software vulnerabilities	✓	–	–
Scanning applications for vulnerabilities	✓	–	–
Inventory of software installed on devices	✓	✓	–
Virtual machines			
Installing Network Agent on a virtual machine	✓	✓	✓
Optimization settings for virtual desktop infrastructure (VDI)	✓	✓	✓
Support of dynamic virtual machines	✓	✓	✓
Other			
Auditing actions on a remote client device by using Windows Desktop Sharing	✓	–	–
Managing device restarts	✓	–	–
Connection Manager	✓	✓	✓
Connection profiles for out-of-office users	✓	✓	✓
Remotely connecting to the desktop of a client device	✓	✓	✓

The following sections are displayed in the distribution point properties, but the corresponding features are not supported by Network Agent for macOS:

- Source of updates
- KSN proxy server
- Windows domains
- Active Directory
- IP ranges
- Advanced
- Statistics

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 **Asset management** → **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 Next Expert View 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 Next Expert View 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 Next Expert View 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.

Replacing third-party security applications

Installation of Kaspersky security applications through Kaspersky Next Expert View may require removal of third-party software incompatible with the application being installed. Kaspersky Next Expert View 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. You can find this option in the Protection deployment wizard. When this option is enabled, Kaspersky Next Expert View 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** task. 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.

Options for manual installation of applications

You can install Network Agent on devices locally without involving Kaspersky Next Expert View. To do this, create a stand-alone installation package for Network Agent as described in the following topic: Creating stand-alone installation packages. Transfer the package to your client device and install it. Once the installation of the Network Agent is completed, you can use the device as a distribution point.

Forced deployment through the remote installation task of Kaspersky Next Expert View

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 Next Expert View—provided that each device has a user account(s) with local administrator rights.

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 distribution points.

You must specify an account that has access to the admin$ share in the settings of the remote installation task.

You can specify target devices either explicitly (with a list), by selecting the Kaspersky Next Expert View 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 Next Expert View feature that ensures network interaction. The following conditions must be met in this case:

- Target devices are accessible 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.

  Also, TCP port 445 is checked to determine the operating system type of the target device before performing a remote installation (if UDP 137 is not available).

  > 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 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 Next Expert View 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.

Devices acting as distribution points must meet the requirements for distribution points. You have to make sure that distribution points are present in each of the isolated subnets hosting target devices.

The free disk space in the partition with the %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit folder must exceed, by many times, the total size of the distribution packages of installed applications.

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 **Discovery & deployment** → **Deployment & assignment** → **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**.

Step 1. Starting Protection deployment wizard

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 way you want to install the selected installation package:

- **Remote installation by Kaspersky Security Center**
- **Remote installation by Microsoft Azure API**

After that, 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.

Step 3. Selecting 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 Kaspersky Security Center Administration Server.

Select the latest version of Network Agent.

Step 4. 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.

Step 5. 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.

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.

Password to uninstall the current Kaspersky application

> 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.

Enter the password in the **Password to uninstall the current Kaspersky application** field if you migrate from one Kaspersky application to another and your current application is password-protected. Note that during the migration, your current Kaspersky application will be uninstalled.

To complete the migration scenario successfully, make sure that the following prerequisites are met:

- You are using the Kaspersky Security Center Network Agent 14.2 for Windows or later.
- You are installing the application on devices running Windows.

Step 6. 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.

Step 7. 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 Next Expert View 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 8. 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.

Step 9. 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 Next Expert View 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 Next Expert View. 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>"
    ```

Step 10. 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.

Network settings for interaction with external services

Kaspersky Next Expert View uses the following network settings for interacting with external services.

Network settings

Network settings	Address	Description
Port: 443 Protocol: HTTPS	activation-v2.kaspersky.com	Application activation.
Port: 443 Protocol: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Updating Kaspersky databases, software modules, and applications.
Port: 443 Protocol: HTTPS	https://downloads.upd.kaspersky.com	• Updating Kaspersky databases, software modules, and applications. • Checking if Kaspersky servers are accessible. Before downloading Kaspersky databases and software modules, Kaspersky Next Expert View 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 Protocol: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Updating Kaspersky databases, software modules, and applications.
Port: 443 Protocol: HTTPS	ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com	Using Kaspersky Security Network.
Port: 443, 1443 Protocol: HTTPS	ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Using Kaspersky Security Network.
Port: 443 Protocol: HTTPS	click.kaspersky.com redirect.kaspersky.com	Following links from the interface.
Port: 80 Protocol: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Public Key Infrastructure (PKI).
Port: 443 Protocol: HTTPS	https://ipm-klca.kaspersky.com	Marketing announcements

Network settings	Address	Description
Port: 443 Protocol: HTTPS	https://tip.kaspersky.com	Responding to threats through Kaspersky Threat Intelligence Portal (when using the Kaspersky Next XDR Optimum functionality).
Port: 443 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).

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 Next Expert View 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 a Linux device and installing Network Agent on a Linux device remotely

Network Agent installation is comprised of two steps:

- A Linux device preparation
- Network Agent remote installation

A Linux device preparation

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. Download the Network Agent installation package by using the application interface or from the Kaspersky website.

   If you need to install Kaspersky Industrial CyberSecurity for Linux Nodes on a device running a Linux operating system with glibc 2.5, you must download one of the following installation packages from the Kaspersky website:

   - klnagent64_16.1.0-5840_amd64_glibc2.5.deb
   - klnagent64-16.1.0-5840.x86_64_glibc2.5.rpm
   - klnagent_16.1.0-5840_i386_glibc2.5.deb
   - klnagent-16.1.0-5840.i386_glibc2.5.rpm

   These installation packages are available for the following operating systems with glibc 2.5:

   - CentOS 5.2 32-bit/64-bit
   - CentOS 5.4 32-bit/64-bit
   - CentOS 6.4 32-bit/64-bit
   - CentOS 6.6 32-bit/64-bit
   - Astra Linux Special Edition RUSB.10015-01 (operational update 1.4) 64-bit

   You must have the Kaspersky Industrial CyberSecurity for Linux Nodes license to get the installation package.

3. 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

4. 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.

      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.

   b. Disable the sudo password for the user account under which the device is to be connected.

   c. 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`

   d. Save the sudoers file and then close it.

   e. 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.

5. 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`.

   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.

   To apply the changed setting, restart the Linux device or execute the following command:

   ```
   sudo systemctl restart systemd-logind.service
   ```

6. 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.

7. 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.

8. 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.

Network Agent remote installation

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 applications using a remote installation task

Kaspersky Next Expert View allows you to install applications on devices remotely, by using remote installation tasks. These 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:

- **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.
- **Specify device addresses manually or import addresses from a list**. In this case, 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.
- **Assign task to an administration group**. In this case, the task is assigned to devices included in an administration group created earlier.

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 Next Expert View.

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 **Asset management** → **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 NetBIOS names, 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.

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:

   - Select how you want to install the selected application:

     - **Remote installation by Kaspersky Security Center**

     - **Remote installation by Microsoft Azure API**

       For more information on how to install applications on Microsoft Azure virtual machines, refer to Remote installation of applications to Azure virtual machines.

   - 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.

- 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 Next Expert View 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 then restart 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 applications 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 options:

  - **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 Next Expert View checks if the Installation utility settings are applicable to the operating system of the client device. If the settings are not applicable, Kaspersky Next Expert View 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, a distribution point automatically determines the device's operating system type, regardless of the **Verify operating system type before downloading** setting.

- **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.

  The **Do not move devices** option is selected by default. For security reasons, you might want to move the devices manually.

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.

   - **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.

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 Next Expert View 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 Next Expert View. 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.

Installing applications on secondary Administration Servers

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.

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 **Asset management** → **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.
4. In the **Task type** list, select the **Start or stop application** 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.

To run the task, select it in the task list, and then click the **Start** button.

Mobile Device Management

Management of mobile device protection through Kaspersky Next Expert View is carried out by using the Mobile Device Management feature. 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 devices of the employees. The protection is provided by the Kaspersky Security for Mobile app installed on the devices. This mobile app ensures protection of mobile devices against web threats, viruses, and other programs that pose threats.

iOS devices

Kaspersky Device Management for iOS ensures protection and control of mobile devices that are connected to Kaspersky Next Expert View.

The Kaspersky Security for iOS app offers the following key features:

- **Web Protection**. This component blocks malicious websites designed to spread malicious code. Web Protection also blocks fake (phishing) websites designed to steal confidential data of the user (for example, passwords for online banking or e-money systems) and access the user's financial info.

- **Jailbreak detection**. When Kaspersky Security for iOS detects a jailbreak, it displays a critical message and informs you about the issue.

For information about protection deployment and management of mobile devices, refer to Basic MDM in Kaspersky Next Expert View (cloud) Help.

Detection and response capabilities

Kaspersky Next Expert View can integrate features of other Kaspersky solutions into the console interface. For example, you can add the detection and response features to the functionality of Kaspersky Next Expert View.

The detection and response solutions are designed to protect an organization's IT infrastructure from complex cyberthreats. The solutions' functionality combines automatic threat detection with the ability to respond to these threats to resist complex attacks, including new exploits, ransomware, fileless attacks, and methods that use legitimate system tools.

Solutions you can integrate

Kaspersky Endpoint Detection and Response Optimum

After a Kaspersky Endpoint Protection Platform (also referred to as EPP) application detects a threat, Kaspersky Next Expert View adds a new alert to the alert list. An alert contains detailed information about the detected threat and enables you to analyze and investigate the threat. You can also visualize the threat by creating a threat development chain graph. The graph describes the deployment stages of the detected attack in time.

As a response, you can choose one of the predefined response actions, for example, move a file to Quarantine, isolate a compromised device from the network, or create an execution prevention rule for an untrusted object.

For information about the solution activation, see the Kaspersky Endpoint Detection and Response Optimum documentation.

Kaspersky Managed Detection and Response

After a Kaspersky EPP application detects a threat, Kaspersky Next Expert View adds a new incident to the incident list. An incident contains detailed information about the detected threat. The MDR Security Operation Center (SOC) analysts of Kaspersky or a third-party company investigate the incidents and offer responses to solve the incidents. You can accept or reject the offered measures manually, or enable the option to auto-accept all of the responses.

For information about the solution activation, see the Kaspersky Managed Detection and Response documentation.

Kaspersky Endpoint Detection and Response Expert

This is a solution for organizations that have a team of SOC analysts. The detected threats are registered as alerts or incidents that can be assigned to SOC analysts for investigation. Kaspersky Endpoint Detection and Response Expert provides you with detailed information on each alert or incident, as well as the tools for alert and incident management, threat hunting, and custom rules development. The SOC analysts or security officers can manually select the response actions, or the predefined automated response measures can be taken.

For information about the solution activation, see the Kaspersky Endpoint Detection and Response Expert documentation.

Interface changes after integrating the detection and response features

The table below lists the changes that the solutions make in the interface of Kaspersky Next Expert View after integration.

Interface changes made by integrated Kaspersky solutions

Solution	Changes in Kaspersky Next Expert View
Kaspersky EDR Optimum	Adds the following elements: • **Alerts** section (**Monitoring** → **Alerts**). The alerts detected by this solution are listed on the **Optimum** tab. • A widget on **Dashboard** (**Monitoring** → **Dashboard**).
Kaspersky MDR	Adds the following elements: • **MDR** section (**Monitoring** → **MDR**). • The **Show MDR features** option (**Settings** → **Interface options** → **Show MDR features**). • A widget on **Dashboard** (**Monitoring** → **Dashboard**).
Kaspersky EDR Expert	Adds the following elements: • **Alerts** section (**Monitoring** → **Alerts**). The alerts detected by this solution are listed on the **Expert** tab. • **Incidents** section (**Monitoring** → **Incidents**). • **Threat hunting** section (**Monitoring** → **Threat hunting**). • **Custom rules** section (**Monitoring** → **Custom rules**). • General settings of Kaspersky EDR Expert (**Settings** → **Integration** → **Kaspersky EDR Expert**). • Widgets on **Dashboard** (**Monitoring** → **Dashboard**).

Data Discovery

This section contains information about Data Discovery.

About Data Discovery

Kaspersky Next Expert View detects critical information in files that are located in Microsoft 365 cloud storages. You can view the information about each detected file—its name, sharing type (private, within the company, or outside the company), and who edited it last.

> This feature is available only if you have activated Kaspersky Next Expert View under a Kaspersky Next EDR Optimum or XDR Expert license.

You can start using the Data Discovery feature when you start Kaspersky Next Expert View Management Console for the first time or after Kaspersky Next Expert View is upgraded to a new version. If you did not start using Data Discovery during the initial or additional setup of Kaspersky Next Expert View, you can do it later. After you start using the feature, connect your Microsoft 365 organization to your workspace.

The Data Discovery widget and table display detections of critical information in files. The widget shows up to 5 detected files and the table shows up to 1000 detections.

From the Data Discovery table, you can export information about all of the current detections to a CSV file.

If you want to stop using the feature, you can disable it. Later, you can enable it again.

> If you delete your workspace after starting the use of Data Discovery, or if you disable the feature and do not want to use it again, you must go to your Microsoft 365 and manually revoke the permissions that you granted to the **Kaspersky Next Expert View – DLP scanner** application.

Categories of information detected by Data Discovery

Kaspersky Next Expert View detects the following categories of critical information:

- Credit/Debit Card Number
- Argentinian Personally Identifiable Information:
  - Argentinian Driver's License
  - Argentinian Identity Card
  - Argentinian Passport
  - Argentinian Unique Taxpayer Number

- Brazilian Personally Identifiable Information:
  - Brazilian Driver's License (CNH)
  - Brazilian Identity Card (RG)
  - Brazilian Individual Taxpayer Registry (CPF)
  - Brazilian Passport
- Chilean Personally Identifiable Information:
  - Chilean Driver's License
  - Chilean Identity Card
  - Chilean Passport
  - Chilean Unique Taxpayer Number
- Colombian Personally Identifiable Information:
  - Colombian Driver's License
  - Colombian Identity Card
  - Colombian Passport
  - Colombian Unique Taxpayer Number (NIT)
- Egyptian Personally Identifiable Information:
  - Egyptian Driver's License
  - Egyptian National Identity Card
  - Egyptian Passport
- Emirati Personally Identifiable Information:
  - Emirates ID
  - Emirati Passport
  - UAE Driver's License
  - UAE Unified Number
- French Personally Identifiable Information:
  - French Driver's License
  - French Identity Card

    - French Passport
    - French Social Security Number
- German Personally Identifiable Information:
    - German Driver's License
    - German Identity Card
    - German Passport
    - German Residence Permit
    - German Social Insurance Number (SIN)
    - German Tax Identification number (TIN)
- Indian Personally Identifiable Information:
    - Indian Driver's License
    - Indian Goods and Services Tax Identification Number
    - Indian Identity Number (Aadhaar)
    - Indian Passport
    - Indian Taxpayer Identification Number
    - Indian Voter ID Card
- Italian Personally Identifiable Information:
    - Italian Driver's License
    - Italian Fiscal Code
    - Italian Identity Card
    - Italian Passport
- Malaysian Personally Identifiable Information
    - Malaysian Identity Card
    - Malaysian Taxpayer Identification Number
    - Malaysian Driver's License
- Mexican Personally Identifiable Information:
    - Mexican Citizen Card (CURP)
    - Mexican Individual Taxpayer Registry (RFC)

    - Mexican Passport
    - Mexican Social Security Number
- Peruvian Personally Identifiable Information
    - Peruvian National Identity Card (DNI)
    - Peruvian Taxpayer Identification Number (RUC)
    - Peruvian Driver's License
    - Peruvian Residence Permit
- Portuguese Personally Identifiable Information:
    - Portuguese Citizen Card
    - Portuguese Driver's License
    - Portuguese Passport
    - Portuguese Social Security Number (NISS)
    - Portuguese Tax Identification Number (NIF)
- Saudi Arabian Personally Identifiable Information:
    - Saudi Arabian Driver's License
    - Saudi Arabian National ID
    - Saudi Arabian Residence Permit
    - Saudi Passport
- South African Personally Identifiable Information
    - South African Passport
    - South African Identity Card
    - South African Tax Reference Number
- Spanish Personally Identifiable Information:
    - Spanish Identity Card
    - Spanish National Insurance Number
    - Spanish Passport
    - Spanish Unique Taxpayer Reference

- Turkish Personally Identifiable Information:
  - Turkish Driver's License
  - Turkish Foreigner ID
  - Turkish Identity Card
  - Turkish Insurance Registration Number (4/a SSK)
  - Turkish Passport
  - Turkish Taxpayer Identification Number
- UK Personally Identifiable Information:
  - UK Driving License
  - UK National Insurance Number
  - UK Passport
  - UK Residence Card
  - UK Tax Identification Number (TIN)
- USA Personally Identifiable Information:
  - US Driver's License
  - US Individual Taxpayer Identification Number (ITIN)
  - US Passport
  - US Social Security Number (SSN)

Starting the use of Data Discovery

You can start using the Data Discovery feature when you start Kaspersky Next Expert View Management Console for the first time or after Kaspersky Next Expert View is upgraded to a new version. If you did not start using Data Discovery during the initial or additional setup of Kaspersky Next Expert View, you can do so as described in this section.

To start using Data Discovery:

1. Open Kaspersky Next Expert View.
2. Do one of the following:
   - In the **Information panel** section, select the **Getting started** tab.
   - In the **Information panel** section, select the **Monitoring** tab.

- In the **Settings** section, click the **Settings** link below **Use of Data Discovery for Microsoft Office 365**.

  The **Data Discovery** page opens.

3. Click **Enable Data Discovery**.

   The **Limitation of Liability Agreement** window opens.

4. Carefully read the Limitation of Liability Agreement, select the check box under the agreement text, and click the **I accept the terms** button if you agree to them.

   If you click the **I decline** button, you will not be able to use Data Discovery.

Data Discovery is enabled.

Next, you must connect your Microsoft 365 organization to your workspace. After that, you will be able to view information about detections.

You can disable this feature later if you decide not to use it.

Accepting the terms and conditions of the Data Discovery Agreement

To accept conditions of the Data Discovery Agreement:

1. Open Kaspersky Next Expert View.

2. Do one of the following:

   - (If the **Data Discovery detections** widget has been added to the dashboard.) In the **Monitoring** → **Dashboard** section, under **Data Discovery detections**, click the **Enable Data Discovery** button.

   - In the **Services** → **Data Discovery** section, click the **Enable Data Discovery** button.

   This opens the **Data Discovery Agreement** window.

3. Carefully read the Agreement, select the check box under the agreement text, and then click the **I accept the terms** button if you agree to them.

   > If you click the **I decline** button, you will not be able to use Data Discovery.

The terms and conditions of the Data Discovery Agreement are accepted.

Kaspersky Next Expert View prompts you to connect your Microsoft 365 organization to your workspace.

Connecting a Microsoft 365 organization to your workspace

After you start using the Data Discovery feature, you must connect your Microsoft 365 organization to your Kaspersky Next Expert View workspace, as described in this section. After that, you will be able to view the Data Discovery detections in Management Console.

To connect a Microsoft 365 organization to your workspace:

1. Open Kaspersky Next Expert View.
2. Do one of the following:

   - In the **Information panel** section, select the **Getting started** tab, and then click **Connect Office 365 organization**.
   - In the **Information panel** section, select the **Monitoring** tab, and then click either the **Connect Office 365 organization** button or the **Connect Office 365 organization** link.

   You are redirected to the Microsoft Online website.
3. Specify the required Microsoft 365 Global Administrator account and accept the granting of the requested permissions.

   The Global Administrator account that you specify must belong to the same Microsoft 365 organization about which you want to view the information. Note that Kaspersky Next Expert View does not store the Global Administrator credentials and uses the acquired consent only.

   You are returned to the Kaspersky Next Expert View.

After the specified credentials are checked and verified, your Microsoft 365 organization will be connected to your Kaspersky Next Expert View workspace. Kaspersky Next Expert View starts the first scan of files that are located in Microsoft 365 cloud storages.

After the scan completes, you can view the detections in the Data Discovery widget and table.

Viewing information about Data Discovery detections

You can view information about Data Discovery detections in a widget and a table. The widget shows up to 5 detected files and the table shows up to 1000 detections.

Data Discovery widget

To view the Data Discovery widget:

1. Open Kaspersky Next Expert View.
2. In the **Information panel** section, click the **Monitoring** tab.
3. If Data Discovery is disabled, enable the feature.

   The Data Discovery widget displays up to 10 detected files.

4. Select or clear the **Private**, **Company**, and **External** check boxes, to view up to 10 detected files shared to the selected audience (privately, within the company, or outside the company).

5. Click the link in the **Data categories** or **File name** column to view detailed information about a detected file.

The widget displays the requested information.

From the widget, you can proceed to the table with the Data Discovery detections.

Data Discovery table

To view the table with the Data Discovery detections:

1. Open Kaspersky Next Expert View.

2. Do one of the following:

   - In the **Information panel** section, click the **Monitoring** tab, and then click the **Go to list of detections** link in the Data Discovery widget.

   - Select the **Security management** → **Data Discovery** section.

3. If Data Discovery is disabled, enable the feature.

   The table displays up to 1000 detected files.

4. Filter the displayed records:

   a. By default, the quick filter is displayed. You can filter the displayed records by the Microsoft 365 service that stores the detected files.

   b. Click **Extended filter** to use the extended filter.

   c. Select values in the drop-down lists:

      - **Detected on**—The period over which files are detected.

      - **Data categories**—Categories of critical information that are detected in the files.

      - **Access type**—The audience to which the files are shared (privately, within the company, or outside the company).

      - **Last edited by**—If you select **Custom**, the **Last edited by** window opens. There, specify a text fragment to find accounts of the users who last edited the detected files.

      - **Service name**—Microsoft 365 service that stores the detected files.

   d. Click **Quick filter** to return to the quick filter.

5. Click the link in the **File name** or **Data categories** column, to view detailed information about a detected file.

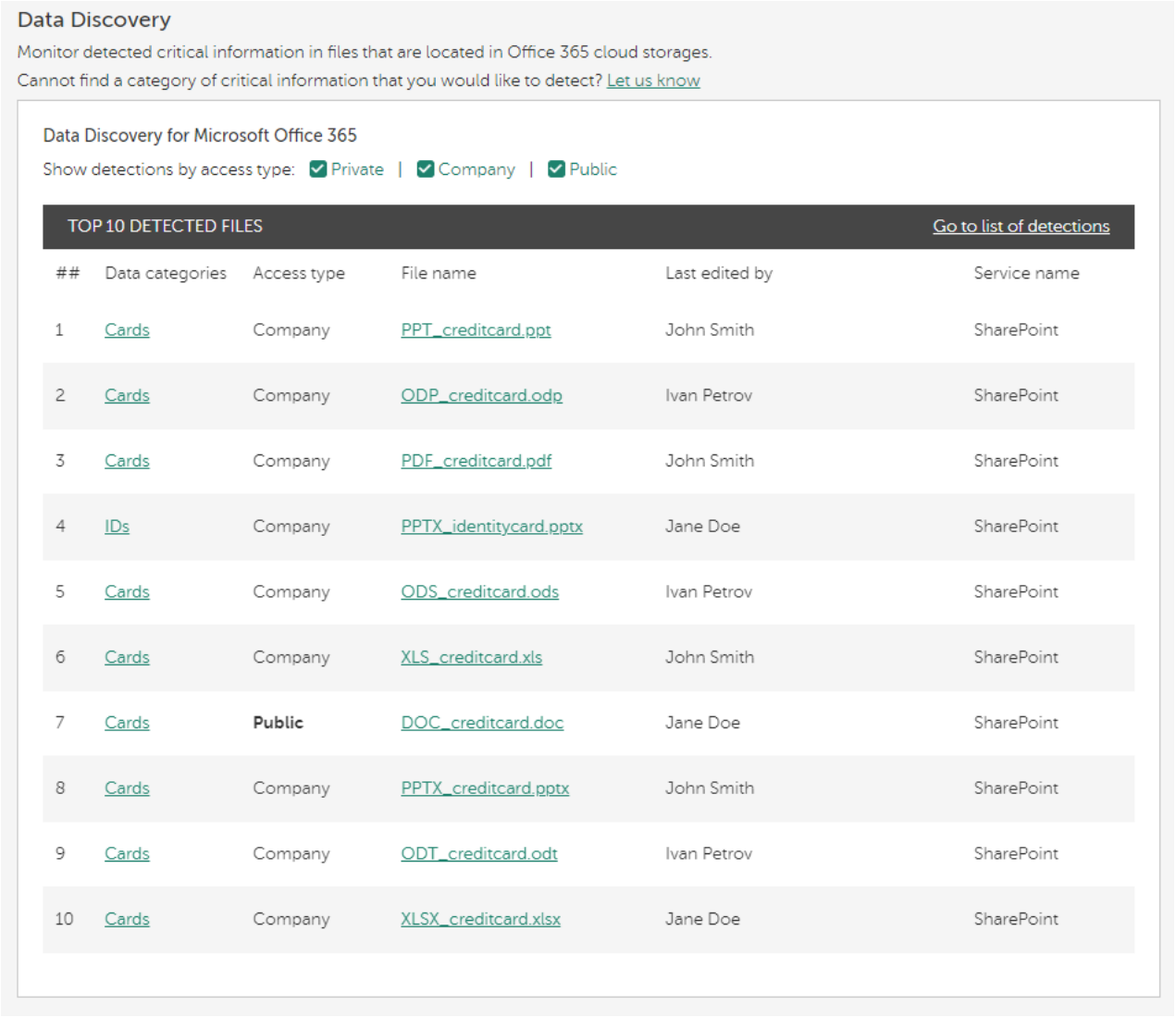
The table displays the requested information.

From the displayed table, you can export information about all of the current detections to a CSV file.

Example of analyzing a Data Discovery detection

This section contains an example of a Data Discovery detection and how you can analyze and process it.

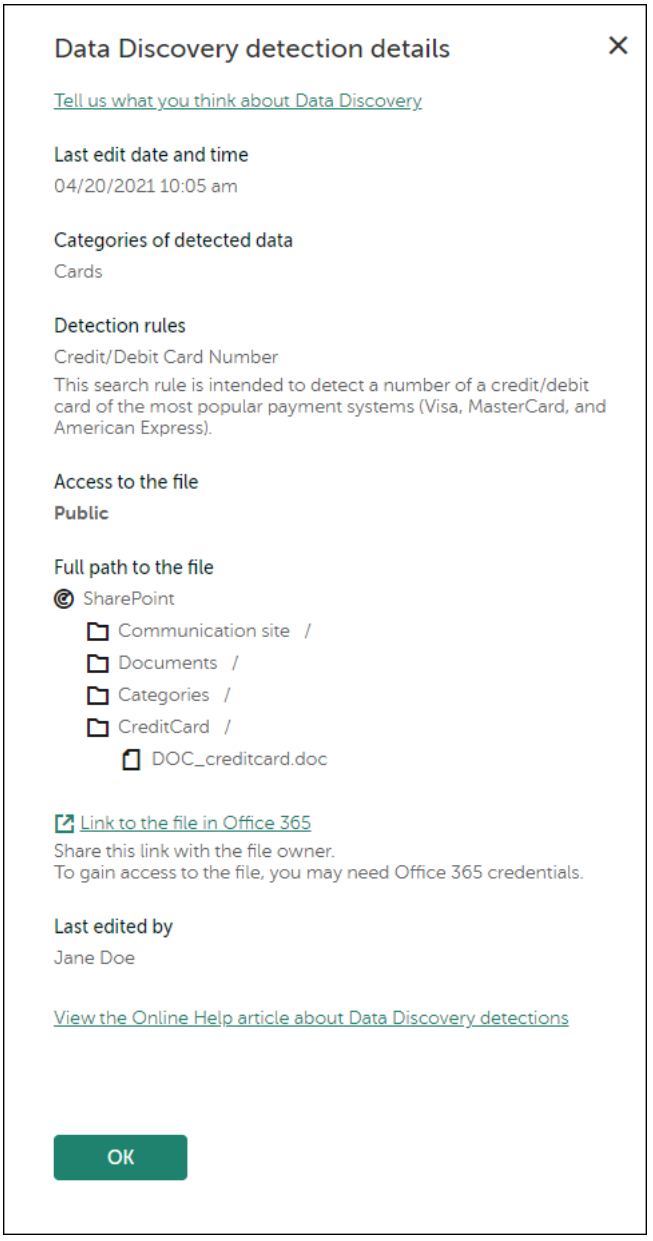
Let's consider that you open the Data Discovery widget (see the figure below) and see a file that is accessible to everyone (the value in the **Access type** column is **Public**).



Data Discovery widget with a file that is accessible to everyone

From the value in the **Data categories** column, you conclude that the file contains credit card details. The value in the **Last edited by** column most often shows the user who configured the accessibility of the file.

By clicking the link in the **Data categories** or **File name** column, you can view detailed information about the detected file (see the figure below).

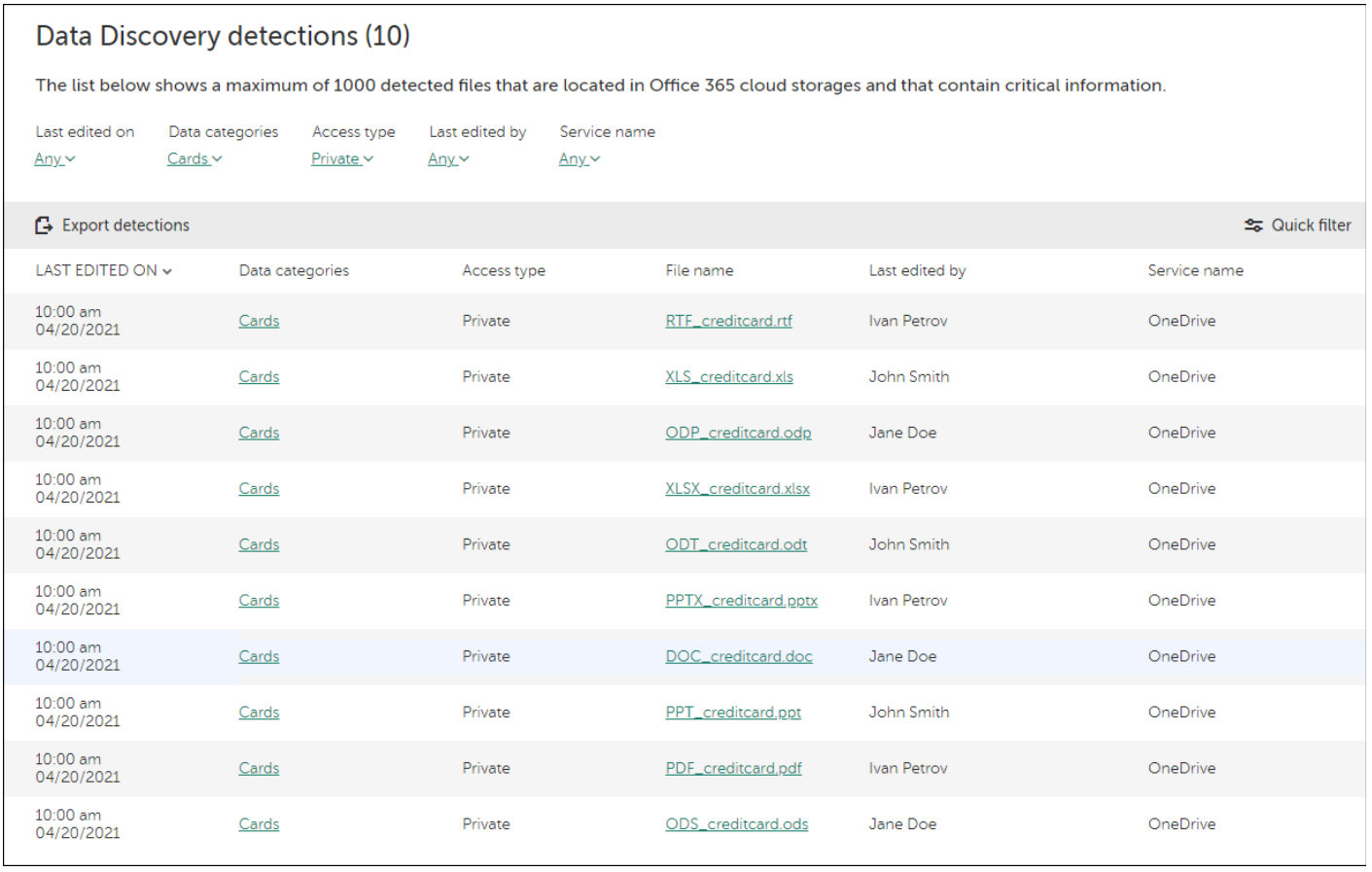


Data Discovery detection details

You can copy either the direct link to the file (**Link to the file in Office 365**) or the structure of the path to it (under **Full path to the file**).

Then you can address the user directly, show him or her the file, and explain that making a file with personal details accessible to everyone may lead to a data breach. You can ask the user to reduce the file audience to the user himself or herself.

Later, after the user follows your advice, you can open the Data Discovery table, apply the filters (if necessary), and see the same document that is now accessible only to its owner (see the figure below).



Data Discovery detections (10)

The list below shows a maximum of 1000 detected files that are located in Office 365 cloud storages and that contain critical information.

Last edited on: Any | Data categories: Cards | Access type: Private | Last edited by: Any | Service name: Any

Export detections | Quick filter

LAST EDITED ON	Data categories	Access type	File name	Last edited by	Service name
10:00 am 04/20/2021	Cards	Private	RTF_creditcard.rtf	Ivan Petrov	OneDrive
10:00 am 04/20/2021	Cards	Private	XLS_creditcard.xls	John Smith	OneDrive
10:00 am 04/20/2021	Cards	Private	ODP_creditcard.odp	Jane Doe	OneDrive
10:00 am 04/20/2021	Cards	Private	XLSX_creditcard.xlsx	Ivan Petrov	OneDrive
10:00 am 04/20/2021	Cards	Private	ODT_creditcard.odt	John Smith	OneDrive
10:00 am 04/20/2021	Cards	Private	PPTX_creditcard.pptx	Ivan Petrov	OneDrive
10:00 am 04/20/2021	Cards	Private	DOC_creditcard.doc	Jane Doe	OneDrive
10:00 am 04/20/2021	Cards	Private	PPT_creditcard.ppt	John Smith	OneDrive
10:00 am 04/20/2021	Cards	Private	PDF_creditcard.pdf	Ivan Petrov	OneDrive
10:00 am 04/20/2021	Cards	Private	ODS_creditcard.ods	Jane Doe	OneDrive

Data Discovery table with applied filters

Exporting information about Data Discovery detections

From the table with Data Discovery detections, you can export information about all of the current detections to a CSV file. For example, you can use a file with detections to prepare a report for your management.

To export information about Data Discovery detections:

1. Proceed to the table with the Data Discovery detections.
2. Click the **Export detections** button.

   The **Export Data Discovery detections** window opens.
3. Click **Export** to confirm the export.

A file with Data Discovery detections is created and automatically downloaded. The file contains the same columns as the table with detections.

Disabling Data Discovery

If you want to stop using Data Discovery, you can disable the feature as described in this section.

To disable Data Discovery:

1. Open Kaspersky Next Expert View.
2. Select the **Settings** section.
   The **General settings of Kaspersky Next Expert View** page is displayed.
3. Click the **Settings** link in the **Use of Data Discovery for Microsoft Office 365** section.
   The **Data Discovery** page opens.
4. Click the **Disable Data Discovery** button.
5. In the confirmation window that opens, click the **Disable** button.

Data Discovery is disabled.

Later, you can enable the feature again.

Discovering networked devices and creating administration groups

This section describes search and discovery of networked devices, as well as creating administration groups for these devices.

Kaspersky Next Expert View enables 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 Kaspersky Next Expert View Administration Server and its secondary Administration Servers.
- Unassigned devices managed by Kaspersky Next Expert View Administration Server and its secondary Administration Servers.

Scenario: Discovering networked devices

You must perform device discovery before the initial deployment 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.

When you complete the scenario, device discovery is set up and will be conducted according to the specified schedule.

Prerequisites

In Kaspersky Next Expert View, device discovery is performed by distribution points. Before you start, do the following:

- Decide which devices will act as distribution points.
- Install Network Agents on the devices that you chose.
- Manually assign the devices to act as distribution points.

Stages

The scenario proceeds in stages:

1. **Choosing types of discovery**

   Decide which type(s) of discovery you want to use regularly.

2. **Configuring polls**

   In the properties of each distribution point, enable and configure the types of network polling that you chose: Windows network polling, domain controller polling, or IP range polling. Make sure that the poll schedule meets the needs of your organization.

   If networked devices are included in a domain, it is recommended to use domain controller polling.

3. **Setting up rules for adding discovered devices to administration groups (optional)**

   New devices that appear on the network are detected as part of network polling. Such devices automatically end up in 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 step, 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.

When a network polling operation is complete, check that the newly discovered devices are arranged according to the configured rules. If no rules are configured, the devices stay in the **Unassigned devices** group.

Network polling

Information about the structure of the network and devices on this network is received by Kaspersky Next Expert View through regular polling of the Windows network, IP ranges, Microsoft Active Directory domain controller and a Samba domain controller. For a Samba domain controller, Samba 4 is used as an Active Directory domain controller. Network polling can be started either manually or automatically according to a schedule.

Based on the results of this polling, Kaspersky Next Expert View updates the list of unassigned devices. You can also configure rules for newly discovered devices to be moved automatically to administration groups.

Kaspersky Next Expert View uses the following methods of network polling:

- *IP range polling*. Kaspersky Next Expert View polls the specified IP ranges using Internet Control Message Protocol (ICMP) packets and compiles a complete set of data on devices within those IP ranges.

- *Windows network polling*. You can run either of the two Windows network polls: fast or full. During a fast poll, Kaspersky Next Expert View only retrieves information from the list of the NetBIOS names of devices in all network domains and work groups. During a full poll, the following information is requested from each device: operating system (OS) name, IP address, DNS name, and NetBIOS name.

- *Domain controller polling*. Information about the Active Directory unit structure and about DNS names of the devices from Active Directory groups is recorded to the Kaspersky Next Expert View database.

Polling results are shown in the **Discovery & deployment** → **Discovery** section separately for the *Windows network polling* and the *Domain controller polling* methods.

Polling results for *IP range polling* are displayed in the **Discovery & deployment** → **Unassigned devices** section.

One device can be shown in more than one detection area. If a device is detected in the HQ domain and its address is 192.168.0.1, the device will appear in both the **Windows domains** section and the **Unassigned devices** section. You can modify network polling settings for each polling method. For example, you may want to modify the polling schedule or to set whether to poll the entire Active Directory forest or only a specific domain.

Windows network polling

About Windows network polling

During a quick poll, the Administration Server only retrieves 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 must be available on the network.
- The Microsoft Computer Browser service must be used, and the primary browser computer must be enabled on the distribution point.
- 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.

Viewing and modifying the settings for Windows network polling

To modify the properties of Windows network polling:

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 that you want to use to poll the network.

   The distribution point properties window opens.

4. Select the **Windows domains polling** section.

5. Enable or disable Windows network polling by using the **Enable network polling** toggle button.

6. Configure the schedule for the quick polling and the full polling.

   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.

7. Save the properties of Windows network polling.

The properties are saved and applied to all of the discovered Windows domains and workgroups.

Domain controller polling

Kaspersky Next Expert View supports domain controller polling only by using a distribution point. You can configure the polling of the following domain controller types:

- Microsoft Active Directory
- Samba

- FreeIPA
- ALD Pro

Kaspersky Next Expert View allows you to poll a Samba domain controller only by using a Linux distribution point. For a Samba domain controller, Samba 4 is used as an Active Directory domain controller.

When you poll a domain controller, 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. Domain controller polling is performed according to a schedule that you set.

Prerequisites

Before you poll a domain controller, ensure that the following protocols are enabled:

- Simple Authentication and Security Layer (SASL)
- Lightweight Directory Access Protocol (LDAP)

Ensure that the following ports are available on the domain controller device:

- 389 for SASL
- 636 for TLS

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.
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 Next Expert View.

Viewing the results of domain controller polling

To view the results of domain controller polling:

1. In the main menu, go to **Discovery & deployment** → **Discovery** → **Domain controllers**.

   The list of discovered organizational units is displayed.

2. Select an organizational unit, and then click the **Devices** button.

   The list of devices in the organizational unit is displayed.

You can search the list and filter the results.

IP range polling

Kaspersky Next Expert View attempts to perform reverse name resolution for every 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 Next Expert View 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. On the networks where Active Directory is used, such a zone is maintained automatically. But on these networks, IP subnet polling does not provide more information than Active Directory polling. Moreover, administrators of small networks often do not configure the reverse lookup zone because it is not necessary for the work of many network services. For these reasons, IP subnet polling is disabled by default.

Initially, Kaspersky Next Expert View gets IP ranges for polling from the network settings of the distribution point device which is used for network polling. If the device address is 192.168.0.1 and the subnet mask is 255.255.255.0, Kaspersky Next Expert View includes the network 192.168.0.0/24 in the list of polling address automatically. Kaspersky Next Expert View polls all addresses from 192.168.0.1 to 192.168.0.254.

It is not recommended to use IP range polling if you use Windows network polling and/or Active Directory polling.

Viewing and modifying the settings for IP range polling

To view and modify the properties of IP range polling:

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 that you want to use to poll the network.

   The distribution point properties window opens.

4. Select the **IP range polling** section.

5. Enable or disable IP polling by using the **Enable range polling** toggle button.

6. Configure the polling schedule. By default, IP polling runs every 420 minutes (seven hours).

7. If necessary, add or modify IP ranges to poll.

   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.

8. Click **OK**.

The properties are saved and applied to all IP ranges.

Configuring a Samba domain controller

Kaspersky Next Expert View 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 Next Expert View 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.

Adding and modifying an IP range

Initially, Kaspersky Next Expert View gets IP ranges for polling from the network settings of the distribution point device which is used for network polling. If the device address is 192.168.0.1 and the subnet mask is 255.255.255.0, Kaspersky Next Expert View includes the network 192.168.0.0/24 in the list of polling address automatically. Kaspersky Next Expert View 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.

To add a new IP range:

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 that you want to use to poll the network.

   The distribution point properties window opens.

4. Select the **IP range polling** section.

5. To add a new IP range, click the **Add** button.

6. In the window that opens, specify the following settings:

   - **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 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.

- **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.

7. Click **OK**.

The new IP range is added to the list of IP ranges.

When the polling is complete, you can view the list of discovered devices by using the **Devices** button. By default, the life span of the polling results is 24 hours and it is equal to the IP address lifetime setting.

Adjustment of distribution points and connection gateways

A structure of administration groups in Kaspersky Next Expert View serves 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 with tags, device locations in Active Directory organizational units, membership in Active Directory security groups, etc.

- 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 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.

Calculating the number and configuration of distribution points

The more client devices a network contains, the more distribution points it requires. Use the tables below to calculate the number of distribution points required for your network.

Make sure that the devices that you intend to use as 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 not available, update Kaspersky databases, software modules, and applications manually or directly from the Kaspersky update servers.

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:

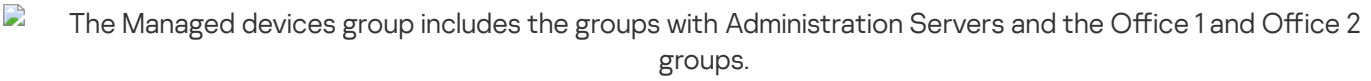
- Building the structure of administration groups taking into account the network topology. The structure of administration groups may not reflect the network topology with absolute precision. A match between the separate parts of the network and certain administration groups would be enough.

- Building the structure of administration groups, without taking the network topology into account. In this case, you must 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.

Assigning distribution points manually

Kaspersky Next Expert View enables you to manually assign devices to act as distribution points. We recommend that you Calculating the number and configuration of distribution points of distribution points required for your network.

Distribution point devices running macOS cannot download updates from Kaspersky update servers.

If one or more devices running 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.

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

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. Click the **Assign** button.

4. 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.

5. Select the administration group that you want to include in the scope of the selected distribution point.

6. Click **Add**.

   The distribution point that you have added will be displayed in the list of distribution points, in the **Distribution points** section.

7. Select the newly added distribution point in the list to open its properties window.

8. 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 Next Expert View 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 Next Expert View, a distribution point can work as a push server for Windows-based and Linux-based devices that are managed by Network Agent. 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 a 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 the scope to which the distribution point will distribute updates (administration groups and / or network location).

  If you want to specify an administration group, click the **Add group** button. In the right pane that opens, select the administration group from the drop-down list, and then click the **Add** button.

  If you want to specify a subnet, click the **Add subnet** button. In the right pane that opens, click the **Add** button, and then specify the subnet name.

  For devices running Windows operating system, the **Automatically assign distribution points within this network location description** toggle switch is displayed. Network location cannot be determined for devices running other operating systems.

- In the **Source of updates** section, you can select a source of updates for the distribution point.

- If your distribution points use proxy server when connecting to the internet, in the **Internet connection settings** section, 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.

    > This feature is not supported by distribution point devices running Linux or macOS.

    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 **I agree to use Kaspersky Security Network** option is 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.

  - **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 if a direct connection cannot be established due to organization of your network. To do this, enable the **Connection gateway** toggle switch.

  By default, this option is disabled.

  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 the polling of Windows domains, domain controller, and IP ranges by the distribution point:

  - **Windows domains polling**

    You can enable device discovery for Windows domains by turning on the **Enable network polling** toggle switch, and then click the **Set full polling schedule** button to set the schedule for the discovery.

    In the window that opens, specify the following settings:

    - **Scheduled start**

You can select one of the following 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 default, the polling runs every five minutes, starting from the current system time.

- **By days of week**

  The polling runs regularly, on the specified days of week, and at the specified time. By default, the polling runs every Friday at 6:00:00 PM.

- **Monthly on selected weekday**

  The polling runs regularly, on the specified days of each month, and at the specified time. By default, no days of month are selected; the default start time is 6:00:00 PM.

- **Start interval (days)**

  Specify what N is equal to (for minutes or days).

  The field is displayed if you selected the **Every N days** or **Every N minutes** schedule option.

- **Starting from**

  Specify when to start the first poll.

  The field is displayed if you selected the **Every N days** or **Every N minutes** schedule option.

- **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.

  This toggle switch is turned off by default. This means that the Administration Server is waiting for the next scheduled poll.

  If you enable the option, Administration Server starts polling immediately after it is switched on.

The section is only displayed for the distribution points running Windows.

- **Domain controller polling**

  You can enable network polling for Active Directory and set the schedule for the poll.

  If you use a Windows distribution point, you can select one of the following options:

  - **Poll current Active Directory domain**.
  - **Poll Active Directory domain forest**.
  - **Poll selected Active Directory domains only**. If you select this option, add one or more Active Directory domains to the list.

  If you perform Active Directory polling by using a Linux distribution point with Network Agent version 15 installed, you can poll only Active Directory domains for which you specify the address and user credentials. Polling of the current Active Directory domain and the Active Directory domain forest is not available.

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**

- **IP range 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.

- In the **Statistics** section you can view statistics on downloading anti-virus databases to the device or statistics on installing packages to the device.

9. Click **OK**.

The selected devices act as distribution points.

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** → **Assets (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 display of 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. Add new distribution points for the administration group by using the **Assign** button or remove the assigned distribution points by using the **Unassign** button.

   > After you click the **Unassign** button, the device will not only be unassigned for the administration group but also will stop acting as a distribution point in general.

Depending on your modifications, the new distribution points are added to the list or existing distribution points are removed from the list.

Using a distribution point as a push server

In Kaspersky Next Expert View, a distribution point can work as a push server for Windows-based and Linux-based devices that are managed by Network Agent. 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 a push server on each of the distribution points. In this case, Administration Server balances the load between the distribution points.

You can use distribution points as push servers to ensure that 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 send packets to the UDP port of Network Agent.

To use a distribution point as a push server:

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 distribution point that you want to use as a push server.
4. In the property list of the selected distribution point, go to the **General** section, and then enable the **Enabled** option.

   The **Push server port** entry field becomes available.

5. In the **Push server port** entry field, specify the port on the distribution point that client devices will use for connection. The default port number is 13295.

   In the Firewall rules, you have to allow outbound network connections between managed devices and the push server port.

6. Click **OK** to exit the distribution point properties window, and then click **Save** to apply changes.

   After you enable the **Enabled** option, the **Do not disconnect from the Administration Server** option is automatically enabled on the distribution point that acts as a push server. This option provides an early connection between Network Agent and the Administration Server.

7. Open the Network Agent policy settings window.

8. Go to **Connectivity** → **Network**, and then enable the **Use distribution point to force connection to the Administration Server** option. Close the lock for this option.

9. Also in the **Network** subsection, you can disable the **Use UDP port** option. The configured push server will provide continuous connectivity between a managed device and the Administration Server instead of sending packets through the UDP port.

10. Click **OK** to close the window.

The distribution point starts acting as a push server. It can now send push notifications to client 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 Next Expert View 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 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, receiving statistics for a managed application, or creating a tunnel. To resolve this issue, if you are not using push servers, you can use the **Do not disconnect from the Administration Server** option to ensure continuous connectivity between a managed device and the Administration Server.

To provide continuous connectivity between a managed device and the Administration Server:

1. Do one of the following:

   - If the managed device accesses the Administration Server directly (that is, not via a distribution point), in the main menu, go to **Asset management** → **Assets (Devices)**, and then click the name of the device with which you want to provide continuous connectivity.

     The property window of the managed device opens.

- If the managed device accesses the Administration Server through a distribution point running in gateway mode, not directly:

  a. Open the Administration Server properties window by clicking the Administration Server name in the main menu.

  Alternately, you can go to the properties of the required Administration Server from the navigation pane. To do so, 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. In the navigation pane that opens, hover the mouse cursor over the name of the required Administration Server, and then click the settings icon (⚙).

  b. On the **General** tab, select the **Distribution points** section.

  c. In the distribution point list, click the name of the required distribution point.

  The properties window of the selected distribution point opens.

2. In the **General** section of the opened properties window, select 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.

Creating administration groups

Initially, the hierarchy of administration groups contains the only administration group named **Managed devices**. When creating a hierarchy of administration groups, you can add devices and virtual machines to the **Managed devices** group and add subgroups. For each administration group, the properties window contains information about policies, tasks, and devices related to the group.

To create an administration group:

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. Select the check box next to the administration group for which you want to create a new subgroup.
3. Click **Add**.
4. Type a name for the new administration group.
5. Click **Add**.

A new administration group with the specified name appears in the administration group hierarchy.

The application allows creation of a hierarchy of administration groups based on the structure of Active Directory or on the structure of the domain network. Also, you can create a structure of groups from a text file.

To create a structure of administration groups:

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. Click the **Import** button.

The New Administration Group Structure Wizard starts. Follow the steps of the wizard.

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. 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.

- **Active rule**

  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 **Copy**.
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.

   - **Active rule**

     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.
- Managed applications installed on client devices, for instance, Network Agent or Administration Server.
- Virtual machines, which are the client devices.
- Information about the Active Directory organizational unit (OU) with the client devices.
- Information about a cloud segment with the client devices.

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 Next Expert View, 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 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.

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 16.2 Network Agent** or **Kaspersky Security Center 16.2 Administration Server**.

  If you do not select any managed application, the condition does not apply.

- **Enabled**

  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.

- **Operating system 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 bit size of the client devices:

  1. In the main menu, go to the **Asset management** → **Assets (Devices)** section.
  2. Click the **Table settings** button ( ) on the right.
  3. Select the **OS architecture** option, and then click the **Save** button.

     After that, the operating system bit size 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** → **Assets (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.

- **Enabled**

  > 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.

- **Enabled**

  > 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 Active Directory 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 Active Directory 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 Active Directory 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 that belong to specific cloud segments:

- **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 you select this option, a device moving rule applies not only to the selected cloud segment, but also to the child objects of this 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 whether a device is detected by API tools:

  - **AWS**. The device is discovered by using AWS API, that is, the device definitely is in the AWS cloud environment.
  - **Azure**. The device is discovered by using Azure API, that is, the device definitely is in the Azure cloud environment.
  - **Google Cloud.** The device is discovered by using the Google API, that is, the device is definitely in the Google cloud environment.
  - **No**. The device cannot be detected by using the AWS, Azure, or Google API, that is, it is either outside the cloud environment or it is in the cloud environment but it cannot be detected by using an API.
  - **No value**. This condition does not apply.

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** → **Assets (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:

     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.
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 the NetBIOS name or DNS name of a device.

    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: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

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** → **Assets (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 **Discovery & deployment** → **Unassigned devices**.

2. If the administration group contains clusters or server arrays, the **Assets (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.

Configuring retention rules for unassigned devices

After Windows network polling is complete, the found devices are placed into subgroups of the Unassigned devices administration group. This administration group can be found at **Discovery & deployment** → **Discovery** → **Windows domains**. The **Windows domains** folder is the parent group. It contains child groups named after the corresponding domains and workgroups that have been found during the poll. The parent group may also contain the administration group of mobile devices. You can configure the retention rules of the unassigned devices for the parent group and for each of the child groups. The retention rules do not depend on the device discovery settings and work even if the device discovery is disabled.

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.

To configure retention rules for unassigned devices:

1. In the main menu, go to **Discovery & deployment** → **Discovery** → **Windows domains**.

2. Do one of the following:

   - To configure settings of the parent group, click the **Properties** button.

     The Windows domain properties window opens.

- To configure settings of a child group, click its name.

  The child group properties window opens.

3. Configure the following settings:

   - **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. By default, this option is also distributed to the child groups. The default time interval is 7 days.

     By default, the option is enabled.

   - **Inherit from parent group**

     If this option is enabled, the retention period for the devices in the current group is inherited from the parent group and cannot be changed.

     This option is available only for child groups.

     By default, this option is enabled.

   - **Force inheritance 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.

4. Click the **Accept** button.

Your changes are saved and applied.

Equipment inventory

The hardware list (**Operations** → **Repositories** → **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 Next Expert View 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 **Operations** → **Repositories** → **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 **Operations** → **Repositories** → **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.

Configuring network protection

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 completed the Kaspersky Next Expert View initial configuration scenario, including the quick start wizard.

When the quick start wizard is running, the following policies and tasks are created 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 of Network Agent)

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. You can also combine these two approaches.

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.

4. **Optimizing the load on endpoint protection applications**

   To avoid decrease in performance, optimize resource consumption by endpoint protection applications.

   For how-to instructions, refer to:

   Kaspersky Endpoint Security for Windows Help

   Kaspersky Endpoint Security for Linux Help

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. You can also differentiate the devices by usage of those devices in Active Directory, or their hardware specifications.

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

This section provides a scenario for a device-centric approach to the centralized configuration of Kaspersky applications installed on 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.

You might also want to consider user-centric security management as an alternative or additional option to the device-centric approach.

Process

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 Next Expert View creates the default policy for Kaspersky Endpoint Security for Windows. If you completed the configuration process by using this wizard, you do not have to create a new policy for this application. Proceed to the manual setup of Kaspersky Endpoint Security policy.

   If you have a hierarchical structure of several administration groups, the child administration groups inherit the policies from the primary Administration Server by default. You can force the inheritance by the child groups 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 located in a specific unit or security group of Active Directory, 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 *Windows*, mark all devices running Windows 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 Windows 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**

   Kaspersky Next Expert View automatically synchronizes the Administration Server with the managed devices several times per hour. 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 Next Expert View 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.

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 Next Expert View 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. Proceed to the manual setup of Kaspersky Endpoint Security policy.

   If you have a hierarchical structure of several administration groups, the child administration groups inherit the policies from the primary Administration Server by default. You can force the inheritance by the child groups 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**

   Kaspersky Next Expert View automatically synchronizes the Administration Server with the managed devices several times per hour. 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 Next Expert View 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.

Network Agent policy settings

To configure the Network Agent policy:

1. In the main menu, go to **Asset management** → **Policies**.
2. Click the name of the Network Agent policy.

   The properties window of the Network Agent policy opens.

See the comparison table detailing how the settings below apply depending on the type of operating system used.

General tab

On this 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**
  - **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 tab

On this tab, you can configure event logging and event notification. Events are distributed according to importance level in the following sections on the **Event configuration** tab:

- **Functional failure**
- **Warning**
- **Info**

In each section, the event type list shows the types of events and the default event storage term on the Administration Server (in days). Clicking the **Properties** button lets you 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.

Application settings tab

Settings

In the **Settings** section, you can configure the Network Agent policy:

- **Distribute files through distribution points only**

  If this option is enabled, client devices receive updates through distribution points only, not directly from update servers.

  If this option is disabled, client devices can receive updates from various sources: directly from update servers and from a local or network folder.

  By default, this option is disabled.

- **Maximum size of event queue, in 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 Windows). 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 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.

  Note that the klmover utility is used only for moving managed devices under management of a virtual Administration Server.

  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. If modification of some settings in this section is prohibited by the Network Agent policy, you cannot modify these settings:

- **Details of installed applications**

- **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 Microsoft Windows Update updates that must be installed on client devices is sent to the Administration Server.

  Sometimes, even if the option is disabled, updates are displayed in the device properties in the **Available updates** section. This might happen if, for example, the devices of the organization had vulnerabilities that could be fixed by these updates.

  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**

Software updates and vulnerabilities

In the **Software updates and vulnerabilities** section, you can configure search of Windows updates, as well as enable scanning of executable files for vulnerabilities. The settings in the **Software updates and vulnerabilities** section are available only on devices running Windows:

- In the **Windows Update search mode** settings group, you can select the update search mode:
  - **Active**

    If this option is selected, Administration Server with support from Network Agent initiates a request from Windows Update Agent on the client device to the update source: Windows Update Servers or WSUS. Next, Network Agent passes information received from Windows Update Agent to Administration Server.

    The option takes effect only if **Connect to the update server to update data** option of the *Find vulnerabilities and required updates* task is selected.

    By default, this option is selected.

  - **Passive**

    If you select this option, Network Agent periodically passes Administration Server information about updates retrieved at the last synchronization of Windows Update Agent with the update source. If no synchronization of Windows Update Agent with an update source is performed, information about updates on Administration Server becomes out-of-date.

    Select this option if you want to get updates from the memory cache of the update source.

  - **Disabled**

    If this option is selected, Administration Server does not request any information about updates.

    Select this option if, for example, you want to test the updates on your local device first.

- **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, this option is disabled.

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.

Windows Desktop Sharing

In the **Windows Desktop Sharing** section, you can enable and configure the audit of the administrator's actions performed on a remote device when desktop access is shared. The settings in the **Windows Desktop Sharing** section are available only on devices running Windows:

- **Enable audit**

  If this option is enabled, audit of the administrator's actions is enabled on the remote device. Records of the administrator's actions on the remote device are logged:

  - In the event log on the remote device.
  - In a file with the syslog extension located in the Network Agent installation folder on the remote device
  - In the event database of Kaspersky Next Expert View

Audit of the administrator's actions is available when the following conditions are met:

- The Vulnerability and patch management license is in use.
- The administrator has the right to start shared access to the desktop of the remote device.

If this option is disabled, the audit of the administrator's actions is disabled on the remote device.

By default, this option is disabled.

- **Masks of files to monitor when read**

  The list contains file masks. When the audit is enabled, the application monitors the administrator's reading files that match the masks and saves information about files read. The list is available if the **Enable audit** check box is selected. You can edit file masks and add new ones to the list. Each new file mask should be specified in the list on a new line.

  By default, the following file masks are specified:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Masks of files to monitor when modified**

  The list contains masks of files on the remote device. When audit is enabled, the application monitors changes made by the administrator in files that match masks, and saves information about those modifications. The list is available if the **Enable audit** check box is selected. You can edit file masks and add new ones to the list. Each new file mask should be specified in the list on a new line.

  By default, the following file masks are specified:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Manage patches and updates

In the **Manage patches and updates** section, you can configure how updates are obtained and distributed to managed devices and how patches are installed: you can enable or disable the **Automatically install applicable updates and patches for components that have the Undefined status** setting.

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 **Connection to Administration Server** settings group, you can specify the following settings:

  - **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 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.

  If the client device runs Windows XP Service Pack 2, the integrated firewall blocks UDP port 15000. This port should be opened manually.

- **Use the distribution point to force a connection to Administration Server**

  Select this option if you selected the **Enabled** option in the distribution point settings window. Otherwise, the distribution point will not act as a push server.

In the **Connection profiles** subsection, no new items can be added to the **Administration Server connection profiles** list so the **Add** button is inactive. The preset connection profiles cannot be modified, either.

In the **Connection schedule** subsection, you can specify the time intervals during which Network Agent sends data to the Administration Server:

- **Connect when necessary**
- **Connect at specified time intervals**

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. The polling settings are available only on devices running Windows. You can use the following options to enable the polling and set its frequency:

- **Windows network**

  If enabled, the distribution point automatically polls the network following the schedule configured by clicking the **Set quick polling schedule** and **Set full polling schedule** links.

  If this option is disabled, the Administration Server does not poll the network.

  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** link.

  If this option is disabled, the distribution point does not poll IP ranges.

  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.

- **User name**

- **Password**

KSN Proxy (distribution points)

In the **KSN Proxy (distribution points)** 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.

  > This feature is not supported by distribution point devices running Linux or macOS.

  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 **I agree to use Kaspersky Security Network** option is 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.

- **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.

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.

Comparison of Network Agent policy settings by operating systems

The table below shows which Network Agent policy settings you can use to configure Network Agent with a specific operating system.

Network Agent policy settings: comparison by operating systems

Policy section	Windows	macOS	Linux
General	✓	✓	✓
Event configuration	✓	✓	✓
Settings	✓	✓ Except the **Use uninstallation password** check box.	✓ Except the **Use uninstallation password** check box.
Repositories	✓	✓ The **Hardware registry details** option is available.	✓ The following options are available: • **Details of installed applications** • **Hardware registry details**
Software updates and vulnerabilities	✓	—	—
Restart management	✓	—	—
Windows Desktop Sharing	✓	—	—
Manage patches and updates	✓	—	—
Connectivity → Network	✓	✓ Except the **Open Network Agent ports in Microsoft Windows Firewall** check box.	✓ Except the **Open Network Agent ports in Microsoft Windows Firewall** check box.
Connectivity → Connection schedule	✓	✓	✓

Policy section	Windows	macOS	Linux
Network polling by distribution points	✓ The following settings are available: • **Windows network** • **IP ranges** • **Domain controllers** (Microsoft Active Directory)	–	✓ The following options are available: • **IP ranges** • **Domain controllers** (Microsoft Active Directory, Samba as an Active Directory)
Network settings for distribution points	✓	✓	✓
KSN Proxy (distribution points)	✓	–	✓

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.

Tasks

This section describes tasks used by Kaspersky Next Expert View.

About tasks

Kaspersky Next Expert View 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 can be performed on the Administration Server and on devices.

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, who uses administration tools, 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.

- *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 multiple 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 OS event log on each device 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), NetBIOS name, or DNS name as the device address.

- 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

You can create a task in the task list. Alternatively, you can select devices in the **Assets (Devices)** list, and then create a new task assigned to the selected devices.

To create a task in the task list:

1. In the main menu, go to **Asset management** → **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.

To create a new task assigned to the selected devices:

In the main menu, go to **Asset management** → **Assets (Devices)**.

The list of managed devices is displayed.

1. 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.
2. Click the **Run task** button, and then select **Create 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.
3. Click the **Finish** button.

The task is created for the selected devices.

Viewing the task list

You can view the list of tasks that are created in Kaspersky Next Expert View.

To view the list of tasks,

In the main menu, go to **Asset management** → **Tasks**.

The list of tasks is displayed. The tasks are grouped by the names of applications to which they are related. For example, the *Uninstall application remotely* task is related to the Administration Server, and the *Find vulnerabilities and required updates* task refers to the Network Agent.

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.

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 **Assets (Devices)** list, and then start an existing task for them.

To start a task manually:

1. In the main menu, go to **Asset management** → **Tasks**.
2. In the task list, select the check box next to the task that you want to start.
3. Click the **Start** button.

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.

To start a task for selected devices:

1. In the main menu, go to **Asset management** → **Assets (Devices)**. The list of managed devices is displayed.

   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.

2. Click the **Run task** button, and then select **Apply existing task**.

   The list of the existing tasks is displayed.

3. 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.

4. 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.

5. Click **Save and start task**.

The selected task is immediately started for the selected devices. The scheduled start settings in the task are not changed.

General task settings and properties

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.

- 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**

  The task is assigned to specific devices. You can specify devices by one of the following methods:

  - Specify the IP address, NetBIOS name, or DNS name of the device.
  - Specify the IP range.

    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.
  - Select devices detected by the Administration Server, including unassigned devices.

    For example, you may want to use this option in a task of installing Network Agent on unassigned devices.

- **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.

- 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.

- Operating system restart settings:

  - **Do not restart**

    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.

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.

- Task scheduling settings:

  > The types of schedule may vary depending on the task.

  - **Start task setting:**

    - **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.

    - **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.

- **When new updates are downloaded to the repository**

  When new updates are downloaded to the distribution point repositories, Kaspersky Next Expert View runs all tasks that have this schedule. Network Agent checks the availability of updates during periodic synchronization between the managed device and the Administration Server (the heartbeat).

  For example, you may want to use this schedule for the Update task related to a security application, such as Kaspersky Endpoint Security.

  If Network Agent on a managed device detects no new updates for 25 hours or longer, then Kaspersky Next Expert View runs on this device all tasks that have this schedule. These tasks are run every hour until new updates are detected. Kaspersky Next Expert View also runs these tasks every hour if there is no connection between the managed device and the distribution point that downloads updates to the repository.

- **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.

The scheduling settings may **depend on the local time zone of the device operating system**.

Correlation between the local time zone of the device operating system and the task start time

Task schedule	Local time is used
Once	No
Every N minutes	No
Every N hours	No
Every N days	Yes
By days of week	Yes
Monthly	Yes
Monthly on selected weekday	Yes
When new updates are downloaded to the repository	Another trigger for running the task (corresponds to the schedule name)
On virus outbreak	Another trigger for running the task (corresponds to the schedule name)
On completing another task	Another trigger for running the task (corresponds to the schedule name)
Immediately	Another trigger for running the task (corresponds to the schedule name)
Manually	Another trigger for running the task (corresponds to the schedule name)

- **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 disabled.

- **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.

- **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.

- **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.

- Notifications:

  - **Store task history** block:

    - **Save all events**
    - **Save events related to task progress**
    - **Save only task execution results**
    - **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 Windows Event Log of each client device.

      By default, this option is disabled.

  - **Notify of errors only**
  - **Notify by email**

- Task scope settings

- **Exclusions from 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 Next Expert View 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 **Asset management** → **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 Next Expert View 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 **Asset management** → **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 NetBIOS names, 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)**.

Viewing task run results stored on the Administration Server

Kaspersky Next Expert View allows you to view the results for group tasks, tasks for specific devices, and Administration Server tasks.

To view the task results:

1. In the task properties window, select the **General** section.

2. Click the **Results** link to open the **Task results** window.

Managing client devices

Kaspersky Next Expert View 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** → **Assets (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 Next Expert View.

- **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**

    Windows domain or workgroup, which contains the device.

  - **DNS name**

DNS domain name of the client device.

- **NetBIOS name**

  Windows network 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.

- 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 Next Expert View.

- **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 Administration Console or in Kaspersky Next Expert View).
    - View the list of recommended fixes for the vulnerability.
    - Manually specify the software updates to fix the vulnerability (in Administration Console or in Kaspersky Next Expert View).
    - 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.

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.
- `Administration 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.
- `Numbers of the Administration Server SSL ports`—Numbers of valid ports for communication with Administration Server when using a secure connection.
- `Numbers of the Administration 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.
- `Administration Server 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.
  - `available`—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.

- `Numbers of 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.
- `Synchronization interval (min)`—Standard interval between synchronizations.
- `Connection timeout (in seconds)`—Connection timeout.
- `Send / receive timeout (in seconds)`—Connection timeout of read-write operations.
- `Device 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:

- `Total number of synchronization requests`—Number of attempts to connect the client device to Administration Server.
- `The number of successful synchronization request`—Number of successful attempts to connect the client device to Administration Server.
- `Total number of synchronizations`—Number of attempts to synchronize the client device settings with the Administration Server settings.
- `The number of successful synchronizations`—Number of successful attempts to synchronize the client device settings with Administration Server.
- `Date/time of the last request for synchronization`—Date and time of the last connection.

You need to use the `Total number of synchronization requests` and `The number of successful synchronization request` 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 `Total number of synchronizations` and `The number of successful synchronization request` parameter values remain unchanged.

For more information on how to troubleshoot issues with connecting Network Agent to Administration Server, refer to Kaspersky Next Expert View FAQ.

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 Next Expert View 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 Next Expert View 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 select one or several devices in the device selection and click the **New task** button to create a task that will be applied to these devices.

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 Windows domain.

- **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 words such as **Window** or **Windows**, you can enter **Windo?**.

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 **Active Directory** subsection, you can configure criteria for including devices into a selection based on their Active Directory data:

- **Device is in an Active Directory organizational unit**

  If this option is enabled, the selection includes devices from the Active Directory organizational unit specified in the entry field.

  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 Active Directory organizational unit.

  By default, this option is disabled.

- **This device is a member of an Active Directory group**

  If this option is enabled, the selection includes devices from the Active Directory 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.

In the **Cloud segments** subsection, you can configure criteria for including devices in a selection according to their respective cloud segments:

- **Device is in a cloud segment**

  If this option is enabled, you can choose devices from the AWS, Azure, and Google cloud segments.

  If the **Include child objects** option is also enabled, the search is run on all child objects of the selected segment.

  Search results include only devices from the selected segment.

- **Device discovered by using the API**

  In the drop-down list, you can select whether a device is detected by API tools:

  - **Yes**. The device is detected by using the AWS, Azure, or Google API.
  - **No**. The device cannot be detected by using the AWS, Azure, or Google API. That is, the device is either outside the cloud environment or it is in the cloud environment but it cannot be detected by using an API.
  - No value. This condition does not apply.

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**

  Name of the device in the Windows network. 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**

  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.

  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.

- **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 Next Expert View:

  - **Yes**. The application includes in the selection devices managed through Kaspersky Next Expert View.
  - **No**. The application includes devices that are not managed via Kaspersky Next Expert View in the selection.
  - **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**

  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*.

  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.

The **Application components** subsection contains the list of components of those applications that have corresponding management plug-ins installed in Kaspersky Next Expert View.

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. Note that the user list is filtered and displays internal users. The search results will 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, you can select the user account for configuring the criterion. Note that the user list is filtered and displays internal users. The search results will include devices on which the specified user logged in to the system at least once.

Exporting the device list from a device selection

Kaspersky Next Expert View 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.

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.

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. Click the name of the required administration group.

   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.

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.

6. Click the **Save** button.

Your changes are saved and applied.

About device statuses

Kaspersky Next Expert View 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 Next Expert View takes into consideration the device's visibility flag on the network (see the table below). If Kaspersky Next Expert View 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. • 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 Virus 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. • Suspended. • Running.

Condition	Condition description	Available values
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.
Restart is required	The device is visible on the network, but an application requires the device restart longer than the specified time interval and for one of the selected reasons.	More than 0 minutes.
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. • 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. • High. • Medium. • Ignore if the vulnerability cannot be fixed. • 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. • 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.	Less 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). • Does not comply with the policy due to an error. • Restart is required when applying the policy. • No encryption policy is specified. • Not supported. • 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. • 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. • Toggle button is on.
Device status defined by application	The status of the device is defined by the managed application.	• Toggle button is off. • 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. • Toggle button is on.

Condition	Condition description	Available values
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. 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. • Toggle button is on.

Kaspersky Next Expert View enables 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.

When Kaspersky Next Expert View assigns a status to a device, for some conditions (see the Condition description column) the visibility flag is taken into consideration. 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.

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. 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 **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**.

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**.

When specified conditions are met, the managed device is assigned the *Warning* status.

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 can switch the device management between the following Administration Servers:

- Primary Administration Server and one of its virtual Administration Servers
- Two virtual Administration Servers of the same primary Administration Server

To change the Administration Server that manages client devices to a different Server:

1. In the main menu, go to **Asset management** → **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, specify the following settings:

   a. In the **Application** drop-down list, select **Kaspersky Next Expert View**.

   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.

      A 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 NetBIOS names, 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, specify an administration group, devices with specific addresses, or a device selection.

5. At the next step, confirm that you agree to the terms of changing the Administration Server for client devices.

6. At the next step, select the virtual Administration Server that you want to use to manage the selected devices.

7. At the **Selecting an account to run the task** step, 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 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.

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.

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.

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 Next Expert View, go to **Discovery & deployment** → **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.

Creating Administration Server connection profiles

To allow out-of-office users to change the method of connecting Network Agent to Administration Server, you have to configure Administration Server connection profiles.

To create a connection profile:

1. In the main menu, go to **Asset management**, and do one of the following:
   - If you want to create a connection profile for a group of managed devices, click **Policies**, and then click **Kaspersky Security Center Network Agent**.
   - If you want to create a connection profile for a specific managed device, click **Assets (Devices)**, and then click the name of the device. In the window that opens, go to the **Applications** tab, and then click **Kaspersky Security Center Network Agent**.

   The properties window of the Network Agent policy opens.
2. Go to the **Application settings** tab, and then go to the **Connectivity** section.
3. In the **Connection profiles** section, click the **Settings** button.
   The **Administration Server connection profiles** subsection displays the table of connection profiles.

   > You cannot view, modify, or delete the **Home Administration Server** and **Offline mode** connection profiles.

4. Click the **Add** button, and then in the window that opens, specify the profile name.

   > The name must be unique. You cannot use the same name for several profiles.

5. If necessary, select the check boxes in the following fields:
   - **Enable out-of-office mode when Administration Server is not available**.
   - **Use proxy server**.

If you select this option, do the following:

- Specify information in the **Address** and the **Port number** fields.
- If necessary, select the **Proxy server authentication** check box, and then specify the user name and the password in the corresponding fields.

6. Click the **Save** button.

The new profile is displayed in the table of connection profiles. You can use it when configuring the **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.

You can edit and delete connection profiles.

To edit a connection profile:

1. In the table of connection profiles click the name of the connection profile that you want to edit.
2. Make all necessary changes, and then click the **Save** button.

The changes are applied to the connection profile.

To delete a connection profile:

1. In the table of connection profiles select the check boxes next to the connection profiles that you want to delete.
2. Click the **Delete** button.

The selected connection profiles are deleted.

About clusters and server arrays

Kaspersky Next Expert View 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 **Assets (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 Next Expert View 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** → **Assets (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 Next Expert View 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.

Device tags

Kaspersky Next Expert View enables you to tag devices. A *tag* is the label of a device 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. You may use manual tagging when you want to tag an individual device. Auto-tagging is performed by Kaspersky Next Expert View in accordance with the specified tagging rules.

Devices are tagged automatically when 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, if your network includes devices running Windows, Linux, and macOS, you can set up a rule that will assign the `[Linux]` tag to all Linux-based devices. Then, you can use this tag when creating a device selection; this will help you sort all Linux-based 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 **Asset management** → **Tags** → **Device tags**.
2. Click **Add**.

   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 **Asset management** → **Tags** → **Device tags**.
2. Click the name of 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 changes.

The updated tag appears in the list of device tags.

Deleting a device tag

To delete a device tag:

1. In the main menu, go to **Asset management** → **Tags** → **Device tags**.
2. In the list, select the device tag 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.

The tag that you have deleted is not removed automatically from auto-tagging rules. After the tag is deleted, it will be assigned to a new device only when the device first meets the conditions of a rule that assigns the tag.

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 **Asset management** → **Tags** → **Device tags**.
2. Click the **View devices** link next to the tag for which you want to view assigned devices.

   You will be redirected to the **Assets (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** → **Assets (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 devices manually

To assign a tag to a device:

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.

To assign a tag to several devices:

1. In the main menu, go to **Asset management** → **Assets (Devices)**.
2. Select the devices to which you want to assign a tag.
3. Click **Tags**, and then select **Assign** from the drop-down list.
4. In the window that opens, select a tag from the drop-down list.
   If necessary, you can select several tags.
   You can also do the following:
   - Edit the name of a tag by clicking the **Edit** (✎) icon.
     Specify the new name of the tag, and then click the **Save** button.

     > Note that the tag will also be renamed in the list of device tags.

   - Delete a tag by clicking the **Delete** (🗑) icon.
     In the window that opens, click **Delete**.

     > Note that the tag will also be deleted from the Administration Server.

5. Click the **Save** button.

The tags are assigned to the selected devices. You can remove the assigned tags.

Removing assigned tags from devices

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.

To remove a tag from a device:

1. In the main menu, go to **Asset management** → **Assets (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 **Yes**.

The tag is removed from the device.

To remove tags from several devices:

1. In the main menu, go to **Asset management** → **Assets (Devices)**.
2. Select the devices whose tags you want to remove.
3. Click **Tags**, and then select **Unassign** from the drop-down list.
4. In the window that opens, select the check boxes next to the tags that you want to remove.

   The window displays all tags assigned to all the devices that you selected at step 2.

5. Click the **Save** button.

The tags are removed from the devices.

Viewing rules for tagging devices automatically

To view rules for tagging devices automatically,

Do one of the following:

- In the main menu, go to **Asset management** → **Tags** → **Auto-tagging rules**.
- In the main menu, go to **Asset management** → **Tags** → **Device tags**, and then click the **Set up auto-tagging rules** link.
- 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 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**.

   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 contain more than 256 characters.
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 contain more than 256 characters. 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 the device name on the Windows network, or device inclusion in a domain or an IP subnet.

     If case sensitive collation is set for the database that you use for Kaspersky Next Expert View, 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.

- **Active Directory**—Presence of the device in an Active Directory organizational unit and membership of the device in an Active Directory group.
- **Applications registry**—Presence of applications of different vendors on the device.

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 **Delete** again.

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. Restart the Network Agent service.

   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.

Quarantine and File backups

Kaspersky anti-virus applications installed on client devices may place files in Quarantine or File backups during device scan.

Quarantine is a special repository for storing files that are probably infected with viruses and files that cannot be disinfected at the time when they are detected.

File backups is designed for storing backup copies of files that have been deleted or modified during the disinfection process.

Kaspersky Next Expert View creates a summarized list of files placed in Quarantine or File backups by Kaspersky applications on the devices. Network Agents on client devices transmit information about the files in Quarantine and File backups to the Administration Server.

Kaspersky Next Expert View does not copy files from repositories to Administration Server. All files are stored in repositories on the devices.

Downloading a file from repositories

Kaspersky Next Expert View enables you to download copies of files that a security application placed in Quarantine or File backups on a client device. Files are copied to the destination that you specify.

You can download files only if one of the following conditions is met: the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, a push server is in use, or a connection gateway is in use. Otherwise, the downloading is not possible.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

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 File backups, 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.

Deleting files from repositories

To delete a file from Quarantine or File backups:

1. In the main menu, go to **Operations** → **Repositories**, and then select one of the following sections:

   - **Quarantine** if you want to delete a file from Quarantine.

   - **File backups** if you want to delete a file from Backup.

2. Depending on the repository that you selected, do one of the following:

   - For the **File backups** section, select file from the list, and then click the **Remove** button.

   - For the **Quarantine** section, delete a file in one of the ways:

     - Select the check box next to the name of the file to be deleted, and then in the toolbar, click the **Delete** button.

     - Click the name of the file to be deleted, and in the details window that opens, in the toolbar, click the **Delete** button.

       In this case, the file is deleted, a corresponding notification is displayed on the screen, and the details window is closed.

   The security application on the client device that had placed files in the repository (Quarantine or File backups) deletes the same files from this repository.

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** → **Assets (Devices)**.
   - If the device belongs to the Unassigned devices group, in the main menu, go to **Discovery & deployment** → **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 application list, 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 Kaspersky Security 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

You can download trace files from a client device only if one of the following conditions is met: the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, a push server is in use, or a connection gateway is in use. Otherwise, the downloading is not possible.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

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.

   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

You can download application settings from a client device only if one of the following conditions is met: the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, a push server is in use, or a connection gateway is in use. Otherwise, the downloading is not possible.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

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

You can download system information from a client device only if one of the following conditions is satisfied: the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, a push server is in use, or a connection gateway is in use. Otherwise, the downloading is not possible.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

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.

> 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

You can download event logs from a client device only if one of the following conditions is satisfied: the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, a push server is in use, or a connection gateway is in use. Otherwise, the downloading is not possible.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

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.
     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 an application and downloading the results

To start diagnostics for an application 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 the application for which you want to run remote diagnostics.

   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 that you want to run on the client device. 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.

Generating a dump file for an application

An application dump file allows you to view the parameters of the application running on a client device at a point in time. This file also contains information about modules that were loaded for an application.

Generating dump files is available only for 32-bit processes running on Windows-based client devices. For client devices running Linux and for 64-bit processes this feature is not supported.

To create a dump file for an application:

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 **Generating the process dump file** section, specify the executable file of the application for which you want to generate a dump file.
4. Click the **Download** button to save the dump file for the specified application.

   If the specified application is not running on the client device, the error message will be displayed.

Remotely connecting to the desktop of a client device

You can obtain remote access to the desktop of a client 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 the connection with the device, you gain full access to information stored on this device and can manage applications installed on it.

Remote connection must be allowed in the operating system settings of the target managed device. For example, in Windows 10, this option is called **Allow Remote Assistance connections to this computer** (you can find this option at **Control Panel** → **System and Security** → **System** → **Remote settings**). If you have a license for the Vulnerability and patch management feature, you can enable this option forcibly when you establish connection to a managed device. If you do not have the license, enable this option locally on the target managed device. If this option is disabled, remote connection is not possible.

To establish remote connection to a device, you must have two utilities:

- Kaspersky utility named klsctunnel. This utility must be stored on your workstation. You use this utility for tunneling the connection between a client device and the Administration Server.

  Kaspersky Next Expert View allows tunneling TCP connections from Administration 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 Administration Console installed to a TCP port on a managed device—if no direct connection is possible between Administration 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.

- Standard Microsoft Windows component named Remote Desktop Connection. Connection to a remote desktop is established through the standard Windows utility mstsc.exe in accordance with the utility's settings.

  Connection to the current remote desktop session of the user is established without the user's knowledge. Once you connect to the session, the device user is disconnected from the session without an advance notification.

To connect to the desktop of a client device, one of the following conditions must be met:

- Client device is a member of an administration group that has a distribution point with the **Do not disconnect from the Administration Server** option enabled.
- In the client device settings, the **Do not disconnect from the Administration Server** option is enabled.

  The maximum total number of client devices with the **Do not disconnect from the Administration Server** option enabled is 300.

To connect to the desktop of a client device:

1. In the main menu, go to **Asset management** → **Assets (Devices)**.
2. Select the check box next to the name of the device to which you want to obtain access.
3. Click the **Connect to Remote Desktop** button.

   The Connect to Remote Desktop window opens.
4. Click the **Download** button to download the klsctunnel utility.
5. Click the **Copy to clipboard** button to copy the text from the text field. This text is a Binary Large OBject (BLOB) that contains settings required to establish connection between the Administration Server and the managed device.

   > A BLOB is valid for 3 minutes. If it has expired, reopen the Connect to Remote Desktop window to generate a new BLOB.

6. Run the klsctunnel utility.

   The utility window opens.
7. Paste the copied text into the text field.
8. If you use a proxy server, select the **Use proxy server** check box, and then specify the proxy server connection settings.
9. Click the **Open port** button.

   The Remote Desktop Connection login window opens.

10. Specify the credentials of the account under which you are currently logged in to Kaspersky Next Expert View.

11. Click the **Connect** button.

    When connection to the device is established, the desktop is available in the Remote Desktop Connection window of Microsoft Windows.

Connecting to devices through Windows Desktop Sharing

You can obtain remote access to the desktop of a client 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.

You can connect to an existing session on a client device without disconnecting the user in this session. In this case, you and the session user on the device share access to the desktop.

To establish remote connection to a device, you must have two utilities:

- Kaspersky utility named klsctunnel. This utility must be stored on your workstation. You use this utility for tunneling the connection between a client device and the Administration Server.

  Kaspersky Next Expert View allows tunneling TCP connections from Administration 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 Administration Console installed to a TCP port on a managed device—if no direct connection is possible between Administration 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.

- Windows Desktop Sharing. When connecting to an existing session of the remote desktop, the session user on the device receives a connection request from you. No information about remote activity on the device and its results will be saved in reports created by Kaspersky Next Expert View.

  You 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.

To connect to the desktop of a client device through Windows Desktop Sharing, the following conditions must be met:

- Microsoft Windows Vista or later is installed on your workstation.

  To check whether the Windows Desktop Sharing feature is included in your Windows edition, make sure that CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} is included in the 32-bit registry.

- Microsoft Windows Vista or later is installed on the client device.

- Kaspersky Next Expert View uses a vulnerability and patch management license.

- The client device is a member of an administration group that has a distribution point with the **Do not disconnect from the Administration Server** option enabled, or this option is enabled in the client device settings.

  Note that the maximum total number of client devices with the **Do not disconnect from the Administration Server** option enabled is 300.

To connect to the desktop of a client device through Windows Desktop Sharing:

1. In the main menu, go to **Asset management** → **Assets (Devices)**.
2. Select the check box next to the name of the device to which you want to obtain access.
3. Click the **Windows Desktop Sharing** button.

   The Windows Desktop Sharing wizard opens.
4. Click the **Download** button to download the klsctunnel utility, and wait for the download process to complete.

   If you already have the klsctunnel utility, skip this step.
5. Click **Next**.
6. Select the session on the device to which you want to connect, and then click the **Next** button.
7. On the target device, in the dialog box that opens, the user must allow a desktop sharing session. Otherwise, the session is not possible.

   After the device user confirms the desktop sharing session, the next page of the wizard opens.
8. Click the **Copy to clipboard** button to copy the text from the text field. This text is a Binary Large OBject (BLOB) that contains settings required to establish connection between the Administration Server and the managed device.

   > A BLOB is valid for 3 minutes. If it has expired, generate a new BLOB.

9. Run the klsctunnel utility.

   The utility window opens.
10. Paste the copied text into the text field.
11. If you use a proxy server, select the **Use proxy server** check box, and then specify the proxy server connection settings.
12. Click the **Open port** button.

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**.

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 Kaspersky Next Expert View Administration Server. This information is stored as a list in the **Rule triggers in Smart Training state** subfolder of the **Repositories** folder. 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 Help.

Viewing the list of 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 **Operations** → **Repositories**.
2. Click the **Rule triggers in Smart Training state** link.

   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.

   - **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.

   - **User name**

     The name of the client device user who run the process that generated the detect.

   - **Processed**

     Date when the anomaly was detected.

- **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).

To view properties of each information element:

1. In the main menu, go to **Operations** → **Repositories**.
2. Click the **Rule triggers in Smart Training state** link.
3. In the window that opens, select the object that you want.
4. Click the **Properties** link.

   The properties window of the object opens and displays information about the selected element.

You can confirm or add to exclusions any element in the list of detections of Adaptive Anomaly Control rules.

To confirm an element,

Select an element (or several elements) in the list of detections and click the **Confirm** button.

The status of the element(s) will be changed to **Confirming**.

Your confirmation will contribute to the statistics used by the rules (for more information, refer to Kaspersky Endpoint Security for Windows documentation).

To add an element as an exclusion,

Select an element (or several elements) in the list of detections and click the **Exclude** button.

The Add exclusion wizard starts. Follow the steps of the wizard.

If you reject or confirm an element, it will be excluded from the list of detections after the next synchronization of the client device with the Administration Server, and will no longer appear in the list.

Adding exclusions from the Adaptive Anomaly Control rules

The Add exclusion wizard enables you to add exclusions from the Adaptive Anomaly Control rules for Kaspersky Endpoint Security for Windows.

To start the Add exclusion wizard through the Adaptive Anomaly Control node:

1. In the main menu, go to **Operations** → **Repositories** → **Rule triggers in Smart Training state**.
2. In the window that opens, select an element (or several elements) in the list of detections, and then click the **Exclude** button.

   You can add up to 1000 exclusions at a time. If you select more elements and try to add them to exclusions, an error message is displayed.

The Add exclusion wizard starts. Proceed through the Wizard by using the **NEXT** button.

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

Initially, the hierarchy of administration groups contains only one administration group called **Managed devices** group. You can add devices and subgroups into the **Managed devices** group.

To create an administration group:

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. In the hierarchy, select the administration group that is to include the new administration group.
3. Click **Add**.
4. In the window that opens, enter a name for the group and click **Add**.

   A new administration group with the specified name appears in the administration group hierarchy.

The application allows creation of a hierarchy of administration groups based on the structure of Active Directory or on the structure of the domain network. Also, you can create a structure of groups from a text file.

To create a structure of administration groups:

1. In the main menu, go to **Asset management** → **Hierarchy of groups**.
2. Click the **Import** button.

   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**, and click the name of the required administration group.
2. In the properties window that opens, go to the **Automatic installation** tab.
3. 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 application applies 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 must 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. On the toolbar, click the **Move** button.
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. In the toolbar, click the **Delete** button.

The administration group is deleted.

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 Next Expert View provides a single policy for each Kaspersky application in an administration group. A policy has one of the following statuses (see the table below):

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.
- You can activate an inactive policy when a specific event occurs. For example, you can enforce stricter anti-virus protection settings during virus outbreaks.
- 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.

You cannot create an Administration Server policy.

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:

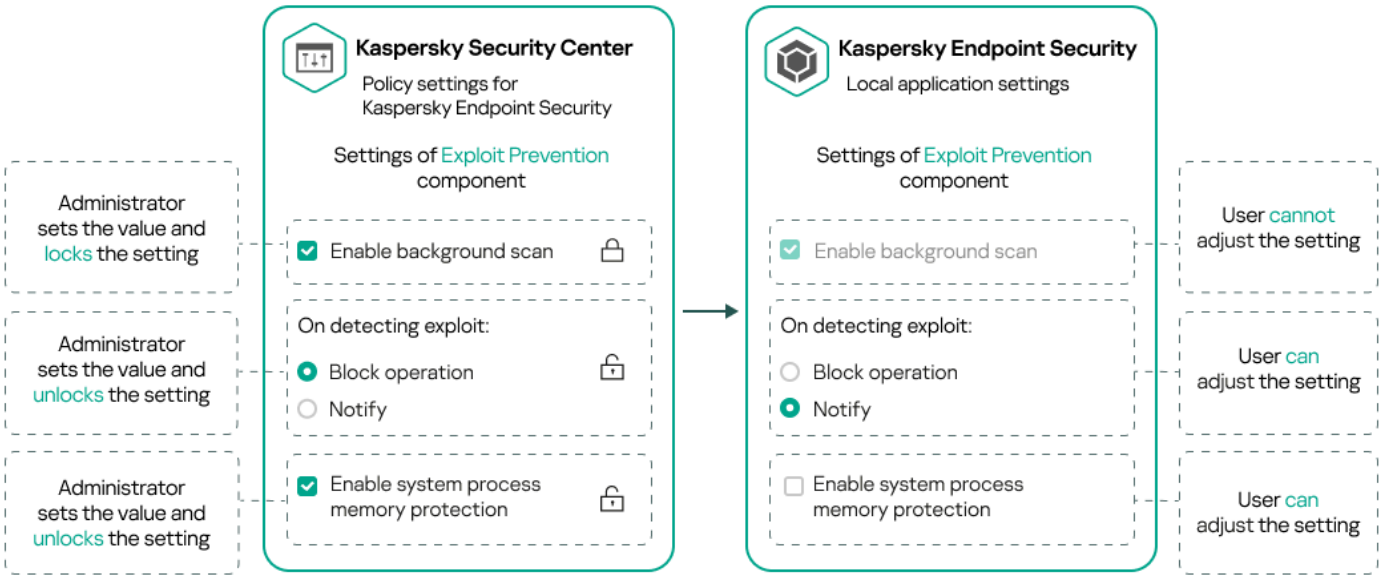
- Locking settings for an administration subgroup policy
- Locking settings of a Kaspersky application on a managed device

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

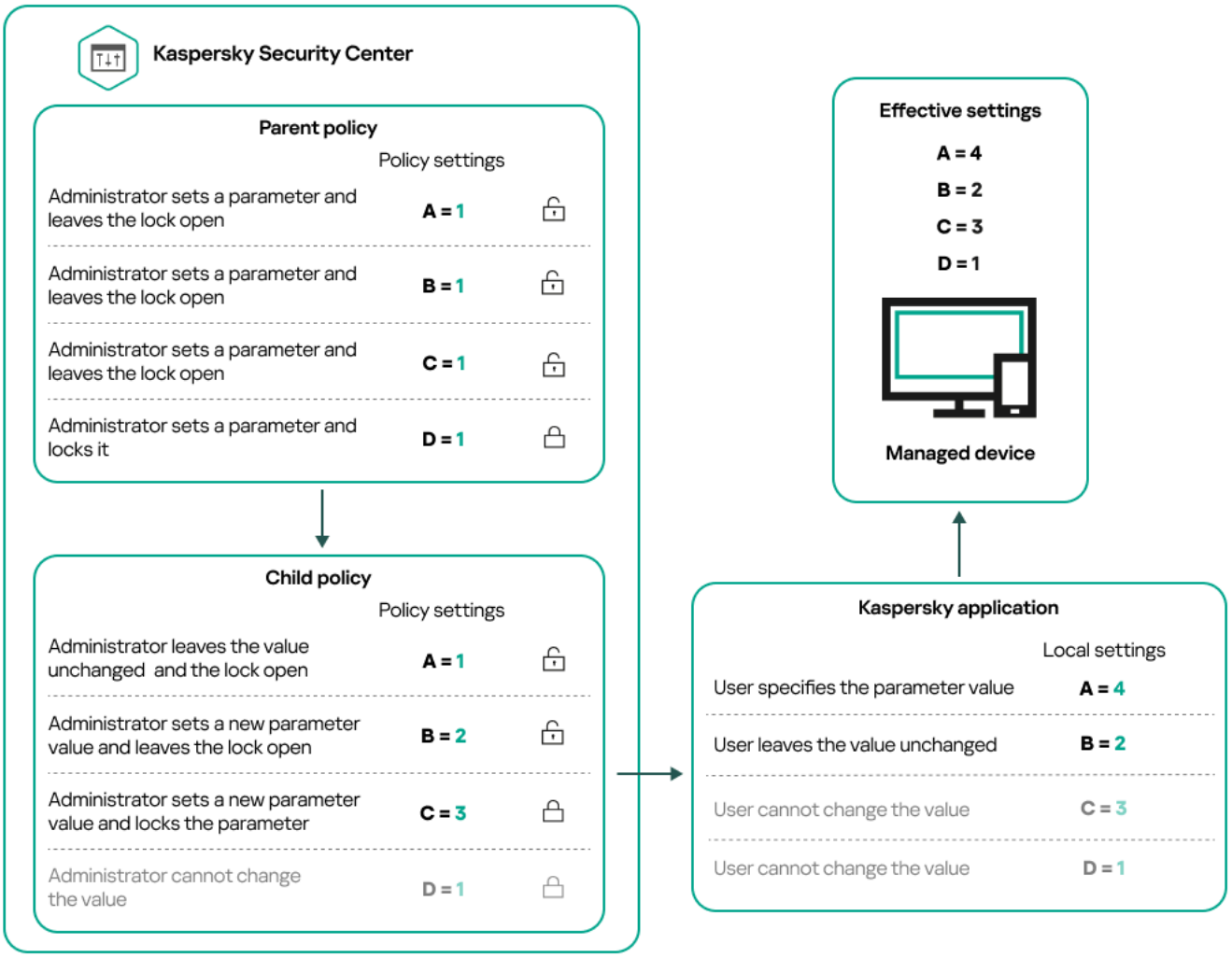
If different devices need different settings, you can organize devices into administration groups.

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).

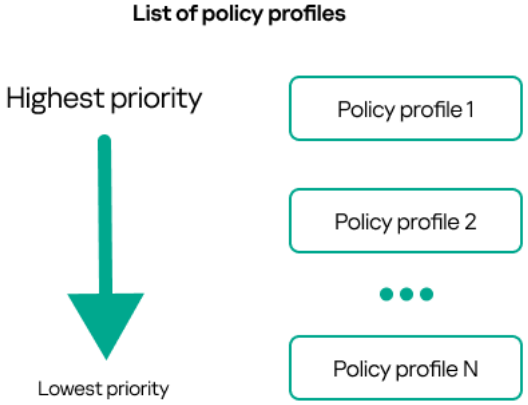


Hierarchy of policies

Policy profiles in a hierarchy of policies

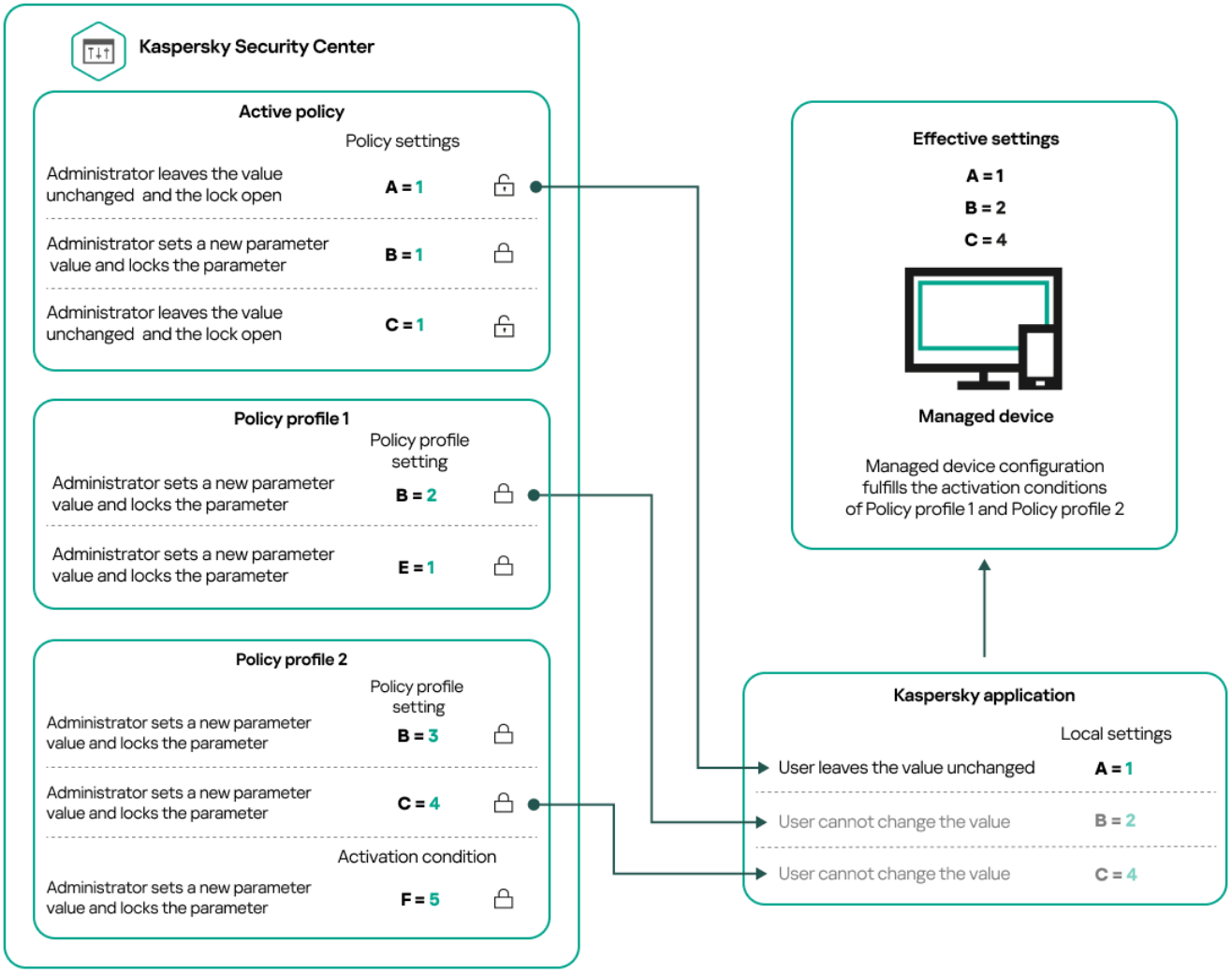
Policy profiles have the following priority assignment conditions:

- 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).

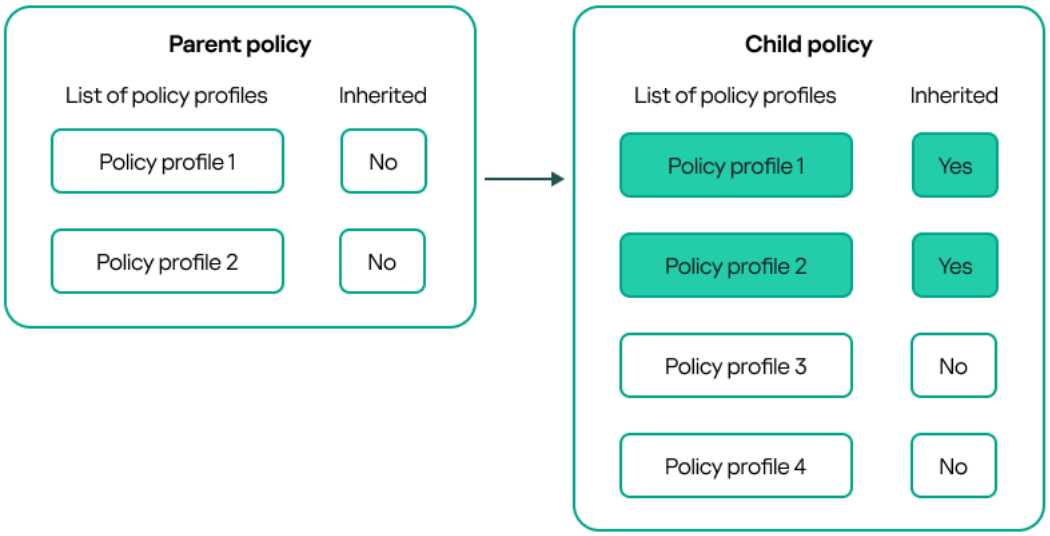


Managed device configuration fulfills activation conditions of several policy profiles

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).

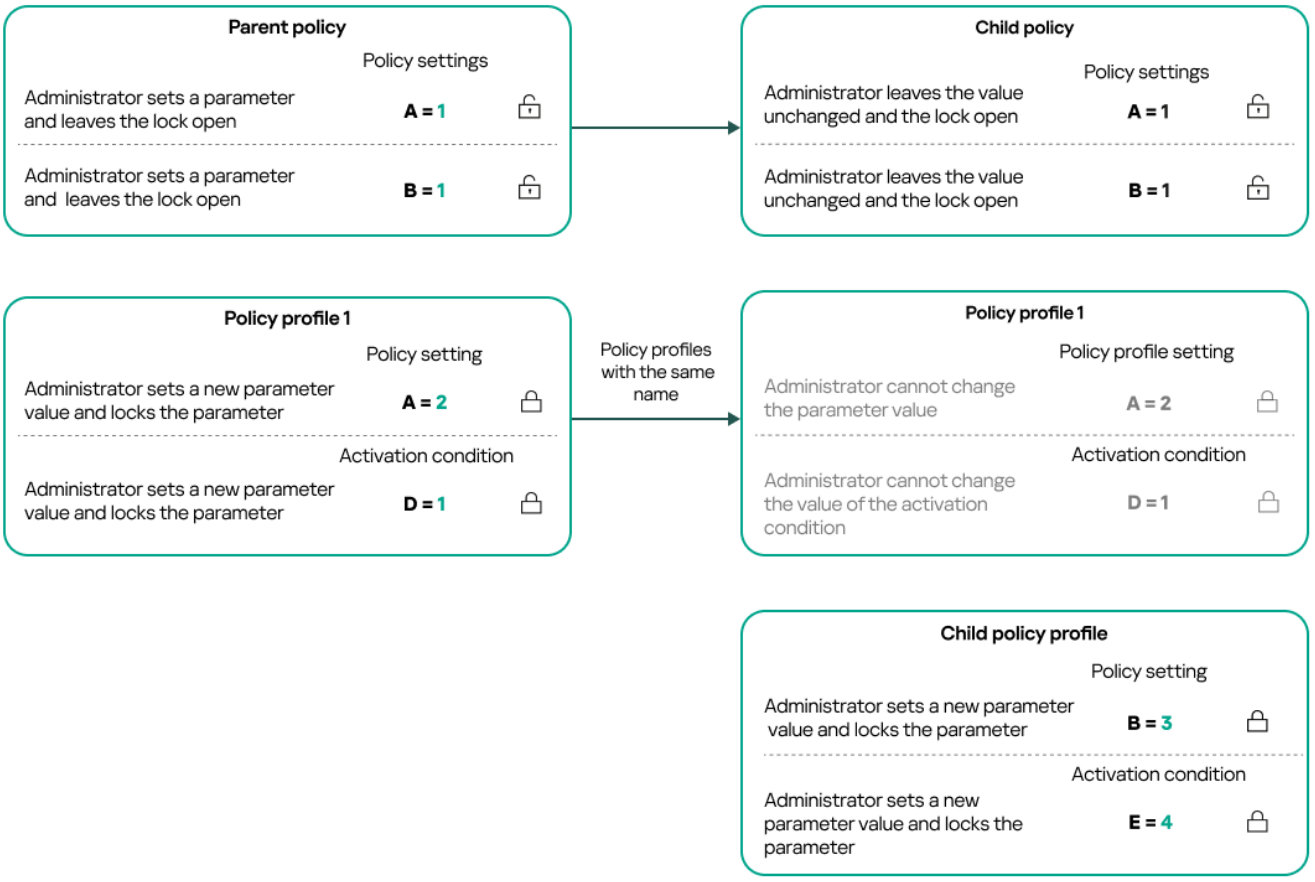


Inheritance of policy profiles

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.

> You cannot create an Administration Server policy.

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.

3. Click **Add**.

   The **Select application** window opens.

4. Select the application for which you want to create a policy.

5. Click **Next**.

   The new policy settings window opens with the **General** tab selected.

6. If you want, change the default name, default status, and default inheritance settings of the policy.

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 application settings depend 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 Windows documentation

   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.

The policy will appear in the list of policies.

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 Windows documentation

   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.

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).

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**
  - **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:

  - **Store in the Administration Server database for (days)**
  - **Store in the OS event log on device**

- **Event notifications**

  You can select if you want to be notified about the event by email.

  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 on the **Email** tab.

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.

Enabling and disabling a policy inheritance option

To enable or disable the inheritance option in a policy:

1. Open the required policy.
2. Open the **General** tab.

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.

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 Next Expert View 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.
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 Next Expert View 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 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)**.

Viewing the policy distribution status chart

In Kaspersky Next Expert View, 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.

3. In the menu that appears, click the **Distribution** link.

   The **<Policy name> distribution results** window opens.

4. In the **<Policy name> distribution results** window that opens, the **Status description (if available)** 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 **Maximum number 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.

Forced synchronization

Although Kaspersky Next Expert View automatically synchronizes the status, settings, tasks, and policies for managed devices, in some cases you need to know for certain, at a given moment, whether synchronization has already been performed for a specified device.

For this feature to work, the **Do not disconnect from the Administration Server** option must be enabled and/or a distribution point must be used as a push server.

Synchronizing a single device

To force synchronization between the Administration Server and a managed device:

1. In the main menu, go to **Asset management** → **Assets (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** → **Assets (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 (...), and 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, you 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** → **Assets (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.

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.

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.

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.

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.

6. Click **Save** to save the profile.

The profile will appear in the list of policy profiles.

Modifying a policy profile

The capability to edit a policy profile is only available for policies of Kaspersky Endpoint Security for Windows.

To modify 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, click the policy profile that you want to modify.

   The policy profile properties window opens.

3. Configure the profile in the properties window:

   - If necessary, on the **General** tab, change the profile name and enable or disable the profile.
   - Edit the profile activation rules.
   - Edit the application settings.

   For details about settings of security applications, please see the documentation of the corresponding application.

4. Click the **Save** button.

The modified settings will take effect either after the device is synchronized with the Administration Server (if the policy profile is active), or after an activation rule is triggered (if the policy profile is inactive).

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).

         Note that the user list is filtered and displays device owners who are internal users.

         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 Next Expert View. 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).

    Note that the user list is filtered and displays device owners who are internal users.

    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 Next Expert View. 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**

    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.

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.

Data encryption and protection

Data encryption reduces the risk of unintentional leakage in case your laptop or hard drive is stolen or lost, or upon access by unauthorized users and applications.

The following Kaspersky applications support encryption:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

You can show or hide some of the interface elements related to the encryption management feature by using the user interface settings.

We do not recommend enabling encryption in VDI.

Encryption of data in Kaspersky Endpoint Security for Windows

You can manage the BitLocker Drive Encryption technology on devices running a Windows operating system for servers or workstations.

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.

You configure encryption by defining policies of Kaspersky Endpoint Security for Windows in Kaspersky Next Expert View. 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 of data in Kaspersky Endpoint Security for Mac

You can use FileVault encryption on devices running macOS. While working with Kaspersky Endpoint Security for Mac, you can enable or disable this encryption.

You can configure encryption by managing Kaspersky Endpoint Security for Mac policies in Kaspersky Next Expert View. Kaspersky Endpoint Security for Mac performs encryption and decryption according to the active policy. For a detailed description of encryption features, see the Kaspersky Endpoint Security for Mac Help.

Viewing the list of encrypted drives

In Kaspersky Next Expert View, 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.

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 the **Encrypted drives** section to generate the report on encryption status of mass storage devices or the report on rights to access encrypted drives.
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 for Windows 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 for Windows Help.

To grant access to an encrypted drive in offline mode:

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 plug-in corresponding to the Kaspersky application that was used to encrypt the selected drive.
6. Follow the instructions provided in the Kaspersky Endpoint Security for Windows Help (see expanding blocks 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.

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 Next Expert View allows you to manage user accounts and groups of accounts. 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 Next Expert View. You can create accounts of internal users. These accounts are used only within Kaspersky Next Expert View.

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. By default, the opened table is filtered by the **Account type** and **Has assigned roles** columns. The table displays internal users or groups that have assigned roles.

If you want to view the table with only the accounts of local users, set the **Account type** filter criteria to **Local**.

If you switch to a secondary Administration Server version 14.2 or earlier, and then open the list of users or security groups, the opened table will be filtered only by the **Account type** column. The filter by the **Has assigned roles** column will not be applied by default. The filtered table will contain all internal users or security groups with the assigned role and without it.

Adding an account of an internal user

In Kaspersky Next Expert View, you can add new users to the workspace. For example, you can assign the added user as a device owner.

To add an account of an internal user:

1. In the main menu, go to **Users & roles** → **Users & groups**.
2. In the **Users** tab, click **Add**.

3. In the **Add users** window that opens, enter the email address of the user that you want to add, and then click **Next**.
4. Review and edit the user details.
5. Click **Finish** to apply the changes.

The account of an internal user is added and appears in the users list.

To edit the information of an internal user's account:

1. In the main menu, go to **Users & roles** → **Users & groups**.
2. In the users list, click the name of the user account that you want to edit.
3. In the window that opens, edit the necessary information.
4. Click **Save** to save changes.

To allow the added internal user to sign in to the Web Console and manage the workspace, you can grant him or her the workspace administrator rights in the Kaspersky Next Expert View. You can also delete an account of an internal user.

Deleting an account of an internal user

To delete an account of an internal user:

1. In the main menu, go to **Users & roles** → **Users & groups**.
2. Select the check box next to the user you want to delete.
3. Click the **Delete** button.
4. Confirm the removal.

The account on an internal user is deleted and cannot be restored.

Assigning workspace administrators

In Kaspersky Next Expert View, you can grant users workspace administrator rights. Workspace administrators can sign in to the Web Console and manage the workspace.

To assign a workspace administrator:

1. In the main menu, go to **Users & roles** → **Users & groups**.
2. In the **Users** tab, click the name of the user that you want to assign a workspace administrator.
3. In the window that opens, enable the **Workspace administrator** toggle switch.
4. Click **Save** to save changes.

To revoke the workspace administrator rights, disable the **Workspace administrator** toggle switch.

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 Next Expert View provides facilities for role-based access to the features of Kaspersky Next Expert View and of managed Kaspersky applications.

You can configure access rights to application features for Kaspersky Next Expert View 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 Next Expert View 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** • Delete device from an administration group: **Write** • Add an administration group to another administration group: **Write** • 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. Access is granted regardless of other rights, even if they prohibit read access to specific objects.
General features: **Basic functionality**	• **Read** • **Write** • **Execute** • **Perform operations on device selections**	• Device moving rules (create, modify, or delete) for the virtual Server: **Write**, **Perform operations on device selections** • Get Mobile (LWNGT) protocol custom certificate: **Read** • Set Mobile (LWNGT) protocol custom certificate: **Write** • Get NLA-defined network list: **Read** • Add, modify, or delete NLA-defined network list: **Write** • View Access Control List of groups: **Read** • View the Kaspersky Event Log: **Read**	• "Download updates to the Administration Server repository" • "Deliver reports" • "Distribute installation package" • "Install application on secondary Administration Servers remotely"	• "Report on protection status" • "Report on threats" • "Report on most heavily infected devices" • "Report on status of anti-virus databases" • "Report on errors" • "Report on network attacks" • "Summary report on mail system protection applications installed" • "Summary report on perimeter defense applications installed" • "Summary report on types of applications installed" • "Report on users of infected devices" • "Report on security issues" • "Report on events" • "Report on activity of distribution points" • "Report on secondary Administration Servers" • "Report on Device Control events"	None

Functional area	Right	User action: right required to perform the action	Task	Report	Other
				• "Report on vulnerabilities" • "Report on prohibited applications" • "Report on Web Control" • "Report on encryption status of managed devices" • "Report on encryption status of mass storage devices" • "Report on file encryption errors" • "Report on blockage of access to encrypted files" • "Report on rights to access encrypted devices" • "Report on effective user permissions" • "Report on rights"	
General features: **Deleted objects**	• **Read** • **Write**	• View deleted objects in the Recycle Bin: **Read** • Delete objects from the Recycle Bin: **Write**	None	None	None
General features: **Event processing**	• **Delete events** • **Edit event notification settings** • **Edit event logging settings** • **Write**	• Change events registration settings: **Edit event logging settings** • Change events notification settings: **Edit event notification settings** • Delete events: **Delete events**	None	None	Settings: • Virus outbreak settings: number of virus detections required to create a virus outbreak event • Virus outbreak settings: period of time for evaluation of virus detections • The maximum number of events stored in the database • Period for storing events from the deleted devices
General features: **Kaspersky software deployment**	• **Manage Kaspersky patches** • **Read** • **Write** • **Execute** • **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" • "Report on Kaspersky software versions" • "Report on incompatible applications"	Installation package: "Kaspersky"

Functional area	Right	User action: right required to perform the action	Task	Report	Other
				• "Report on versions of Kaspersky software module updates" • "Report on protection deployment"	
General features: **Key management**	• **Export key file** • **Write**	• Export key file: **Export key file** • Modify Administration Server license key settings: **Write**	None	None	None
General features: **Enforced report management**	• **Read** • **Write**	• Create reports regardless of their ACLs: **Write** • 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 Administration Servers**	None	None	None
General features: **User permissions**	**Modify object ACLs**	• Change Security properties of any object: **Modify object ACLs** • Manage user roles: **Modify object ACLs** • Manage internal users: **Modify object ACLs** • Manage security groups: **Modiobject ACLs** • Manage aliases: **Modify object ACLs**	None	None	None
General features: **Virtual Administration Servers**	• **Manage virtual Administration Servers** • **Read** • **Write** • **Execute** • **Perform operations on device selections**	• Get list of virtual Administration Servers: **Read** • Get information on the virtual Administration Server: **Read** • Create, update, or delete a virtual Administration Server: **Manage virtual Administration Servers** • Move a virtual Administration Server to another group: **Manage virtual Administration Servers** • Set administration virtual Server permissions: **Manage virtual Administration Servers**	None	"Report on results of installation of third-party software updates"	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
System management: Connectivity	• **Start RDP sessions** • **Connect to existing RDP sessions** • **Initiate tunneling** • **Save files from devices to the administrator's workstation** • **Read** • **Write** • **Execute** • **Perform operations on device selections**	• Create desktop sharing session: **The right to create desktop sharing session** • Create RDP session: **Connect to existing RDP sessions** • Create tunnel: **Initiate tunneling** • Save content network list: **Save files from devices to the administrator's workstation**	None	"Report on device users"	None
System management: Hardware inventory	• **Read** • **Write** • **Execute** • **Perform operations on device selections**	• Get or export hardware inventory object: **Read** • Add, set or delete hardware inventory object: **Write**	None	• "Report on hardware registry" • "Report on configuration changes" • "Report on hardware"	None
System management: Network access control	• **Read** • **Write**	• View CISCO settings: **Read** • Change CISCO settings: **Write**	None	None	None
System management: Operating system deployment	• **Deploy PXE servers** • **Read** • **Write** • **Execute** • **Perform operations on device selections**	• Deploy PXE servers: **Deploy PXE servers** • View a list of PXE servers: **Read** • Start or stop the installation process on PXE clients: **Execute** • Manage drivers for WinPE and operating system images: **Write**	Create installation package upon reference device OS image	None	Installation package: "OS Image"
System management: Vulnerability and patch management	• **Read** • **Write** • **Execute** • **Perform operations on device selections**	• View third-party patch properties: **Read** • Change third-party patch properties: **Write**	• Perform Windows Update synchronization • Install Windows Update updates • "Fix vulnerabilities" • "Install required updates and fix vulnerabilities"	"Report on software updates"	None
System management: Remote installation	• **Read** • **Write** • **Execute** • **Perform operations on device selections**	• View third-party Vulnerability and patch management based installation package properties: **Read** • Change third-party Vulnerability and patch management based installation	None	None	Installation packages: • "Custom application" • "VAPM package"

Functional area	Right	User action: right required to perform the action	Task	Report	Other
		package properties: **Write**			
System management: **Software inventory**	• **Read** • **Write** • **Execute** • **Perform operations on device selections**	None	None	• "Report on installed applications" • "Report on applications registry history" • "Report on status of licensed applications groups" • "Report on third-party software license keys"	None

Predefined user roles

User roles assigned to Kaspersky Next Expert View 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 and configure the required rights yourself. Some of the predefined user roles available in Kaspersky Next Expert View can be associated with specific job positions, for example, **Auditor**, **Security Officer**, **Supervisor** (these roles are present in Kaspersky Next Expert View starting from the version 11). 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). 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: • **General features**: • **Basic functionality** • **Event processing** • **Hierarchy of Administration Servers** • **Virtual Administration Servers** • **System management**: • **Connectivity** • **Hardware inventory** • **Software inventory** Grants the **Read** and **Write** rights in the **General features: Encryption key management** functional area.
Administration Server Operator	Grants the **Read** and **Execute** rights in all of the following functional areas: • **General features**: • **Basic functionality** • **Virtual Administration Servers** • **System management**: • **Connectivity** • **Hardware inventory** • **Software inventory**
Auditor	Permits all operations in the following functional areas, in **General features**: • **Access objects regardless of their ACLs** • **Deleted objects** • **Enforced report management** You can assign this role to a person who performs the audit of your organization.
Installation Administrator	Permits all operations in the following functional areas: • **General features**: • **Basic functionality** • **Kaspersky Lab software deployment** • **License key management** • **System management**: • **Deploy operating system** • **Vulnerability and patch management** • **Remote installation** • **Software inventory** Grants **Read** and **Execute** rights in the **General features: Virtual Administration Servers** functional area.

Role	Description
Installation Operator	Grants the **Read** and **Execute** rights in all of the following functional areas: • **General features**: • **Basic functionality** • **Kaspersky software deployment** (also grants the **Manage Kaspersky Lab patches** right in this area) • **Virtual Administration Servers** • **System management**: • **Deploy operating system** • **Vulnerability and patch management** • **Remote installation** • **Software inventory**
Kaspersky Endpoint Security Administrator	Permits all operations in the following functional areas: • **General features: Basic functionality** • Kaspersky Endpoint Security area, including all features Grants the **Read** and **Write** rights in the **General features: Encryption key management** functional area.
Kaspersky Endpoint Security Operator	Grants the **Read** and **Execute** rights in all of the following functional areas: • **General features: Basic functionality** • Kaspersky Endpoint Security area, including all features
General administrator	Permits all operations in functional areas, *except* for the following areas, in **General features**: • **Access objects regardless of their ACLs** • **Enforced report management** Grants the **Read** and **Write** rights in the **General features: Encryption key management** functional area.
Main Operator	Grants the **Read** and **Execute** (where applicable) rights in all of the following functional areas: • **General features**: • **Basic functionality** • **Deleted objects** • **Operations with Administration Server** • **Kaspersky application deployment** • **Virtual Administration Servers** • **Mobile Device Management: General** • **System management**, including all features • Kaspersky Endpoint Security area, including all features
Mobile Device Management Administrator	Permits all operations in the following functional areas: • **General features: Basic functionality** • **Mobile Device Management: General**
Mobile Device Management Operator	Grants the **Read** and **Execute** rights in the **General features**: **Basic functionality** functional area. Grants **Read** and **Send only information commands to mobile devices** in the **Mobile Device Management**: **General** functional area.
Security Officer	Permits all operations in the following functional areas, in **General features**: • **Access objects regardless of their ACLs** • **Enforced report management** Grants the **Read**, **Write**, **Execute**, **Save files from devices to the administrator's workstation**, and **Perform operations on device selections** rights in the **System management: Connectivity** functional area. You can assign this role to an officer in charge of the IT security in your organization.

Role	Description
Senior Security Analyst	Grants the **Read** right in the **General features**: **Basic functionality** functional area. Grants the **Read**, **Write**, **Execute**, **Save files from devices to the administrator's workstation**, and **Perform operations on device selections rights in the System management**: **Connectivity** functional area. Grants the access rights to the Kaspersky Endpoint Detection and Response Expert solution.
Self Service Portal User	Permits all operations in the **Mobile Device Management: Self Service Portal** functional area. This feature is not supported in Kaspersky Security Center 11 and later version.
Supervisor	Grants the **Read** right in the **General features**: **Access objects regardless of their ACLs** and **General features**: **Enforced report management** functional area. 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) 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) 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**
   - **Asset management → 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.

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 steps 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.

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, user 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 user 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 user groups and the selected administration group are added to the scope of the 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 user groups that you want to add to the user role scope.
7. Click the **Assign role** button to close the window.
8. Close the role properties window.

The selected users or user groups and the selected administration group are added to the scope of the 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 scope of the user role, 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 click **OK** 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.

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 **New group**.

3. In the **New group** window, specify the following settings for the new security group:

   - **Name**

   - **Description**

4. Click **OK** to save the changes.

A new security group is added to the security group list.

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.

Adding user accounts to an internal group

You can add only accounts of internal users to an internal group.

To add user accounts to an internal 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 group.
3. Click the **Assign group** button.
4. In the **Assign group** window that opens, select the group to which you want to add user accounts.
5. Click the **Assign** button.

The user accounts are added to the group. You can also add internal users to a group by using the group settings.

Deleting a security group

You can delete only internal security groups.

To delete a user group:

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Groups** tab.
2. Select the check box next to the user group that you want to delete.
3. Click **Delete**, and then confirm the deletion in the opened window.

The user group is deleted.

Configuring ADFS integration

To allow the users registered in Active Directory (AD) in your organization to sign in to Kaspersky Next Expert View, you must configure integration with Active Directory Federation Services (AD FS).

Kaspersky Next Expert View supports AD FS 3 (Windows Server 2016) or a later version. AD FS must be published and available on the internet. As the service communication certificate AD FS uses publicly trusted certificate.

To change AD FS integration settings, you must have the access right to change user permissions.

Before you proceed, make sure that you completed Active Directory polling.

To configure AD FS integration:

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **AD FS integration settings** section.

3. Copy the callback URL.

   You will need this URL to configure the integration in AD FS Management Console.

4. In AD FS Management Console, add a new application group, and then add a new application by selecting the **Server application** template (the names of the Microsoft interface elements are provided in English.).

   AD FS Management Console generates client ID for the new application. You will need the client ID to configure the integration in Kaspersky Next Expert View.

5. As a redirect URI, specify the callback URL that you copied in the Administration Server properties window.

6. Generate a client secret. You will need the client secret to configure the integration in Kaspersky Next Expert View.

7. Save the properties of the added application.

8. Add a new application to the created application group. This time select the **Web API** template.

9. On the **Identifiers** tab, to the **Relying party identifiers** list, add the client ID of the server application that you added before.

10. On the **Client Permissions** tab, in the **Permitted scopes** list, select the **allatclaims** and **openid** scopes.

11. On the **Issuance Transform Rules** tab, add a new rule by selecting the **Send LDAP Attributes as Claims** template:

    a. Name the rule. For example, you can name it 'Group SID'.

    b. Select **Active Directory** as an attribute store, and then map **Token-Groups as SIDs** as a LDAP attribute to 'Group SID' as an outgoing claim type.

12. On the **Issuance Transform Rules** tab, add a new rule by selecting the **Send Claims Using a Custom Rule** template:

    a. Name the rule. For example, you can name it 'ActiveDirectoryUserSID'.

    b. In the **Custom rule** field, type:

    ```
    c:[Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
    Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
    ("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
    ";objectSID;{0}", param = c.Value);
    ```

13. In Kaspersky Next Expert View, open again the **AD FS integration settings** section.

14. Switch the toggle button to the **AD FS integration Enabled** position.

15. Click the **Settings** link, and then specify the file that contains the certificate or several certificates for the federation server.

16. Click the **AD FS integration settings** link, and then specify the following settings:

    - **Issuer URL**

      The URL address of the federation server working in your organization.

      In particular, Kaspersky Next Expert View adds '/.well-known/openid-configuration' to the issuer URL address and tries to open the resulting URL address (issuer_URL/.well-known/openid-configuration) to discover the issuer configuration automatically.

    - **Client ID**

      Client ID that the federation server generates to identify Kaspersky Next Expert View. You can find the Client ID in AD FS Management Console in the properties window of the server application that corresponds to Kaspersky Next Expert View.

    - **Client secret**

      You generate a client secret in AD FS Management Console when you specify the properties of the server application that corresponds to Kaspersky Next Expert View.

    - **Domain to authenticate users from**

      The members of the domain that you select will be able to sign in to Kaspersky Next Expert View with their domain account credentials. The domain names appear in the list after you complete the network polling.

    - **Field name for user SID in ID token**

      Name of the field that refers to the user SID in the ID token. The field name is required to identify the user in Kaspersky Next Expert View. By default, this field in the ID token is called 'primarysid'.

    - **Field name for array of SIDs of user's groups in ID token**

      Name of the field that refers to the array of SIDs of Active Directory security groups in which the user is included. By default, this field in the ID token is called 'groupsid'.

17. Save the settings.

The integration with AD FS is complete. To sign in to Kaspersky Next Expert View with an AD account credentials, use the link provided in the **AD FS integration settings** section (**Login link to Kaspersky Next with**

AD FS).

After you sign in to Kaspersky Next Expert View with an AD account credentials, the following restrictions are imposed:

- The **Data Discovery** section of the main menu is not available.
- The **Manage user account** item is not available in the upper pane.
- You cannot switch between workspaces.

When you sign in to Kaspersky Next Expert View through AD FS for the first time, the console might respond with a delay.

Configuring integration with Microsoft Entra ID

You have to configure integration with Microsoft Entra ID to allow the users in your organization to sign in to Kaspersky Next Expert View with their Microsoft Entra ID account credentials.

Integration with Microsoft Entra ID is available for the primary Administration Server only. You cannot configure the integration for secondary or virtual Administration Servers.

Configuring integration settings

To configure integration with Microsoft Entra ID:

1. In the main menu, click the Administration Server name.
   The Administration Server properties window opens.
2. On the **General** tab, select the **Microsoft Entra ID** section.
3. Turn on the **Microsoft Entra ID integration** toggle button.
4. Copy the links from the following fields:
   - **Callback URL**
   - **Front-channel logout URL**
     You will need these URLs to register Kaspersky Next Expert View in the Microsoft Entra ID tenant.
   - **Login URL**
     You will need this URL to allow users to sign in to the Kaspersky Next Expert View workspace with their Microsoft Entra ID credentials after the integration with Microsoft Entra ID is complete.

5. Sign in to the Microsoft Entra admin center, and then select the tenant of your organization.

   You must have the Global administrator or the Application administrator role in the tenant.

6. In the main menu, go to **Identity** → **Applications** → **App registrations**, and then click the **New registration** button.

7. In the window that opens, do one of the following:

   - Specify a name for the Kaspersky Next Expert View application.
   - In the **Supported account types** section, select the **Accounts in this organizational directory only (<tenant_name> only - Single tenant)** option.
   - In the **Redirect URI** section, select **Web** from the drop-down list, and then enter the callback URL that you copied from Kaspersky Next Expert View at step 4.

8. Click the **Register** button.

   The Kaspersky Next Expert View application is registered in Microsoft Entra ID, and the application overview page opens.

9. If necessary, add Kaspersky Next Expert View to the list of applications.

   The users will be able to open Kaspersky Next Expert View by clicking its name in the list of applications in My Apps and Office 365 Launcher, without using the login URL.

10. Copy the **Application (client) ID** and the **Directory (tenant) ID**, and save them in any convenient way.

    You will need these IDs when filling in the mandatory fields in Kaspersky Next Expert View at step 14.

11. In the menu of the Kaspersky Next Expert View application, go to the **Authentication** section, and then enter the URLs that you copied from Kaspersky Next Expert View at step 4:

    - In the **Web** section, click the **Add URI** button, and then enter the login URL.
    - In the **Front-channel logout URL** section, enter the front-channel logout URL.

12. In the menu of the Kaspersky Next Expert View application, go to the **Certificates & secrets** section, and then do the following:

    a. Go to the **Client secrets** tab, and then click the **New client secret** button.

    b. In the window that opens, specify any description for the client secret, and then select the period after which the secret expires.

    We recommend that you copy the date after which the secret expires, in any convenient way, to rotate the secrets in a timely manner.

    a. Then click the **Add** button.

       The created secret is displayed on the **Client secrets** tab.

b. Copy the information from the **Value** column.

> We strongly recommend that you copy the information immediately after creating the client secret.

13. In the menu of the Kaspersky Next Expert View application, go to the **Token configuration** section, and then do the following:

    - Add the **onprem_sid** optional claim:

      a. Click the **Add optional claim** button.

      b. In the window that opens, select the **ID** token type, and then in the **Claim** column, select the check box next to the **onprem_sid**.

      c. Then click the **Add** button.

      The **onprem_sid** optional claim is displayed on the **Optional claims** page.

    - Add the **preferred_username** optional claim:

      a. Click the **Add optional claim** button.

      b. In the window that opens, select the **Access** token type, and then in the **Claim** column, select the check box next to the **preferred_username**.

      c. Then click the **Add** button.

      The **preferred_username** optional claim is displayed on the **Optional claims** page.

14. In the menu of the Kaspersky Next Expert View application, go to the **API permissions** section, and then add the permissions:

    - **User.Read.All**
    - **User.Export.All**
    - **GroupMember.Read.All**
    - **Directory.Read.All**

    To add a permission, do the following:

    a. Click the **Add a permission** button, and then select the **Microsoft APIs** tab.

    b. Select **Microsoft Graph** → **Application permissions**, and then select the permission you want to add.

    c. Click the **Add permission** button.

    The four permissions are added and displayed on the **Configured permissions** page.

    d. Click the **Grant administrator's consent for <tenant_name>** button, then click **Yes** in the displayed window to confirm consent to the permissions you added.

15. Go back to Kaspersky Next Expert View, and on the **General** tab, fill in the following mandatory fields:

    - **Tenant ID**. The **Directory (tenant) ID** that you copy at step 10.
    - **Client ID**. The **Application (client) ID** that you copy at step 10.
    - **Client secret**. The value that you copy at step 12.

16. Click the **Check connection** button to check if the settings are correct, and then after the **Connected** status is displayed, click the **Save** button.

The integration settings are saved, and the integration with Microsoft Entra ID is configured.

Ensuring that the users are added

After you configure the integration with Microsoft Entra ID, you have to do the following:

1. In the Kaspersky Next Expert View main menu, go to **Users & roles** → **Users & groups** to make sure that the users and groups from Microsoft Entra ID are added to Kaspersky Next Expert View.

   If the users and groups in your Microsoft Entra ID tenant are synchronized from the Active Directory of your organization, and Active Directory polling is configured, then the users and groups are already added to Kaspersky Next Expert View as a result of Active Directory polling.

   Otherwise, you have to enable and run Microsoft Entra ID polling to add the users and groups from your Microsoft Entra ID tenant to Kaspersky Next Expert View.

2. Assign necessary roles to the users and groups.

   When assigning roles to a user on a virtual Administration Server, in the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab. If you select the **Groups** tab, and then assign roles to the group where the user is a member, the user will not be able to log in to Kaspersky Next Expert View.

3. Send the login URL that you copied at step 4 to the users. They will enter this URL to **sign in to the Kaspersky Next Expert View workspace by using their Microsoft Entra ID credentials**.

   When a user signs out of the Microsoft Entra ID account that was used for authentication in Kaspersky Next Expert View, and Kaspersky Next Expert View is open on a different tab or window of the same browser, the session also ends for Kaspersky Next Expert View and the user signs out of the console automatically.

   If Kaspersky Next Expert View is open in a different browser or on different devices, the session continues when the user signs out of the Microsoft Entra ID account.

To sign in to Kaspersky Next Expert View with Microsoft Entra ID account credentials, users must be able to sign in to their Microsoft Entra ID account.

Limitations

When you sign in to Kaspersky Next Expert View with Microsoft Entra ID credentials, the following restrictions are imposed:

- The **Data Discovery** section of the main menu is not available.
- The **Manage user account** item is not available in the upper pane.
- You cannot switch between workspaces.

Enabling Microsoft Entra ID polling

You have to enable Microsoft Entra ID polling to add the users from your Microsoft Entra ID to Kaspersky Next Expert View.

To enable Microsoft Entra ID polling:

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the **General** tab, select the **Microsoft Entra ID** section.
3. In the **User discovery** section, turn on the **Microsoft Entra ID polling** toggle button.
4. If you want to change the default polling schedule, click the **Schedule settings** button, specify the polling frequency and time in the window that opens, and then click the **Save** button.

   Microsoft Entra ID polling will run according to the schedule that you configure.

5. If you want to run Microsoft Entra ID polling immediately, click the **Run now** button.

   The users are loading. When the users are loaded, the Microsoft Entra ID polling is finished.

6. Click the **Save** button.

The Microsoft Entra ID polling is complete, and the users from your Microsoft Entra ID are added to Kaspersky Next Expert View.

Adding Kaspersky Next Expert View to the list of applications

You can allow users to open Kaspersky Next Expert View by clicking its name in the list of applications, without entering the login URL. The application list is available in My Apps and Office 365 Launcher.

To add Kaspersky Next Expert View to the list of applications:

1. In the Microsoft Entra admin center main menu, go to **Identity** → **Applications** → **App registrations**, and then on the **All applications** tab, select the Kaspersky Next Expert View application that you have previously registered in Microsoft Entra ID.

2. In the menu of Kaspersky Next Expert View, select the **Branding & properties** section, and then do the following:

   a. In the **Home page URL** field, enter the login URL.

   b. If necessary, in the **Upload new logo** field, add an image that will be used as the application icon in the list of applications.

   c. Click the **Save** button.

3. In the Microsoft Entra admin center main menu, go to **Identity** → **Applications** → **Enterprise applications**, and then select Kaspersky Next Expert View.

   The application overview page opens.

4. In the menu of Kaspersky Next Expert View, select the **Properties** section, and then do the following:

   a. Set the following options to **Yes**:

   - **Enabled for users to sign-in?**

     This action is necessary only if the option is not set to **Yes** by default.

   - **Visible to users?**

   b. Click the **Save** button.

5. In the menu of Kaspersky Next Expert View, select the **Users and groups** section, and then do the following:

   a. Click the **Add user/group** button, and then click the link below **Users and groups**.

   b. In the window that opens, select users and groups, and then click the **Save** button.

   The window is closed.

   c. Click the **Assign** button.

Kaspersky Next Expert View is available in My Apps and Office 365 Launcher for the selected users. The users can open Kaspersky Next Expert View by clicking its name in the list, without entering the login URL.

Assigning a user as a device owner

For information about assigning a user as a mobile device owner, see Kaspersky Security for Mobile 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 **Add**.

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** → **Assets (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 Linux device owner after installation of Network Agent

To allow the user to register as a Linux device owner:

1. In the Kaspersky Next Expert View, go to **Discovery & deployment** → **Deployment & assignment** → **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.

The user will be registered as a device owner.

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 Next Expert View 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.

Adding a revision description

You can add a description for the revision to simplify the search for revisions in the list.

To add a description for a revision:

1. In the object's properties window, open the **Revision history** tab.
2. In the list of object revisions, select the revision for which you need to add a description.
3. Click the **Edit description** button.

   The **Description** window opens.
4. In the **Description** window, enter some text for the revision description.

   By default, the object revision description is blank.
5. Save the revision description.

The description is added for the revision of the object.

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 number of the revision to which you have to roll back changes.

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.

Viewing and saving a policy revision

Kaspersky Next Expert View allows you to view which modifications were made to a policy over a certain period, as well as save information about these modifications in a file.

Viewing and saving a policy revision are available if the corresponding management web plug-in supports this functionality.

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.

   If the revision size is more than 10 MB, you will not be able to view it by using Kaspersky Next Expert View. 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. 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).

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).

To view a policy revision:

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 pane that is displayed:

     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 Next Expert View. 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.

For the policies of Kaspersky Endpoint Security for Windows and Kaspersky Endpoint Security for Mac, the report on revision comparison will not contain information about the policy profiles.

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 enables you to use Kaspersky reputation databases to retrieve information about applications installed on client devices.

If you participate 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 Next Expert View. 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.

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 update or upgrade 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 Next Expert View checks if the KSN 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 the level of security is maintained for the managed devices.

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

Enabling and disabling KSN

To enable 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 settings** section.

3. Switch the toggle button to the **Use Kaspersky Security Network Enabled** position.

   KSN is enabled.

   If the toggle button is enabled, client devices send patch installation results to Kaspersky. When enabling this toggle button, you should read and accept the terms of the KSN Statement.

4. Click the **Save** button.

To disable 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 settings** section.

3. Switch the toggle button to the **Use Kaspersky Security Network Disabled** position.

   KSN is disabled.

   If this toggle button is disabled, client devices will send no patch installation results to Kaspersky.

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 settings** 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 automatically displayed when you open Kaspersky Next Expert View. 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. You can view and accept the updated KSN Statement 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 KSN proxy server. 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 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.

To check whether the Linux-based distribution point works as KSN proxy server:

1. On the distribution point device, display the list of running processes.

2. In the list of running processes, check whether the `/opt/kaspersky/ksc64/sbin/ksnproxy` process is running.

If `/opt/kaspersky/ksc64/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.

Deletion of objects

You can delete objects, including the following:

- Policies
- Tasks
- Installation packages
- Virtual Administration Servers
- Users

- Security groups
- Administration groups

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 Next Expert View 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 BitLocker Drive 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 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.

> 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 Next Expert View 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.

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 Next Expert View 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. This maintenance ensures that protection of the managed devices remains firm against a range of threats, including viruses, network attacks, and phishing attacks.

There are several schemes that you can use to install updates to Kaspersky Next Expert View components and security applications. Choose one or more schemes that meet the requirements of your network best.

The scenario below describes the update scheme that implies downloading updates to the distribution point repositories. If the managed devices do not have a connection to the distribution points, consider updating Kaspersky databases, software modules, and applications manually or directly from the Kaspersky update servers.

When you complete this scenario, the following results occur:

- Kaspersky Next Expert View components are updated automatically or only when you designate the *Approved* status for the updates.
- Kaspersky security applications, Kaspersky databases, and software modules are updated according to the schedule that you specified. By default, Kaspersky security applications install only those updates that you approve.

You can configure the update process to download and install updates in either of two ways:

- Automatically

  In this case you have to perform this scenario only once. You will have to schedule the *Download updates to the repositories of distribution points* task (if any) and the Update tasks for the Kaspersky security applications, and keep the default update settings that are in the Network Agent properties.

- Manually

  You can configure the update process to run the *Download updates to the repositories of distribution points* task (if any) and the Update tasks for the Kaspersky security applications manually. You can also configure Network Agent to install updates for the Kaspersky Next Expert View components only when you designate the *Approved* status for the updates.

Prerequisites

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 Next Expert View. When performing that scenario, you assigned an appropriate amount of distribution points in accordance with the number of managed devices and the network topology.

2. Created and configured all required policies, policy profiles, and tasks according to the scenario of configuring network protection.

Stages

Configuration of regular updating of Kaspersky databases and applications proceeds in stages:

1. **Creating the task for downloading updates to the repositories of distribution points**

   Create the *Download updates to the repositories of distribution points* task. When this task is run, Kaspersky Next Expert View downloads the updates to the distribution points directly from Kaspersky update servers.

   How-to instructions: Creating the task for downloading updates to the repositories of distribution points

2. **Configuring 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 can download updates only from a local resource or directly from Kaspersky update servers.

   If you want the managed devices to receive updates only from the distribution points, enable the **Distribute files through distribution points only** option in the Network Agent policy.

3. **Optimizing the update process by using diff files (optional)**

   Enabling this feature results in decrease in the traffic between the 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 repositories of distribution points* task.

   How-to instructions: Using diff files for updating Kaspersky databases and software modules

4. **Defining which updates to install**

   By default, the downloaded software updates have the *Undefined* status. Change the status to *Approved* or *Declined* to define if this update should be installed on networked devices. The approved updates are always installed. The undefined updates can only be installed on Network Agent and other Kaspersky Next Expert View components in accordance with the Network Agent policy settings. The updates for which you set *Declined* status will not be installed on devices.

How-to instructions:

- About update statuses
- Approving and declining software updates

5. **Configuring automatic installation of updates and patches for Kaspersky Next Expert View components**

   By default, the downloaded updates and patches for Network Agent and other Kaspersky Next Expert View components are installed automatically. If you have left the **Automatically install applicable updates and patches for components that have the Undefined status** option enabled in the Network Agent properties, then all updates will be installed automatically after they are downloaded to the repository (or several repositories). 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*.

   How-to instructions: Enabling and disabling automatic updating and patching for Kaspersky Next Expert View components

6. **Configuring automatic installation of updates for the security applications**

   Create the Update tasks for the managed applications to provide timely updates to the applications, software modules and Kaspersky databases, including anti-virus databases. We recommend that you select the **When new updates are downloaded to the repository** option when configuring the task schedule. This will ensure that new updates are installed as soon as possible.

   By default, updates for the managed applications are installed only after you change the update status to *Approved*. For Kaspersky Endpoint Security for Windows, you can change the update settings in the Update task.

   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.

   How-to instructions: Automatic installation of Kaspersky Endpoint Security updates on 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 Next Expert View 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 Next Expert View, and management web plug-ins is not supported.

   How-to instructions: Approving and declining software updates

Upon completion of the scenario, you can proceed to monitoring the network status.

About updating Kaspersky databases, software modules, and applications

To be sure that the protection of your 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 Next Expert View 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 Next Expert View components and security applications

Kaspersky experts handle all the necessary updates for Kaspersky Next Expert View and its components, as well as for managed Kaspersky applications. You cannot perform these updates manually

Depending on the configuration of your network, the following schemes of downloading and distributing the required updates to the managed devices can be used:

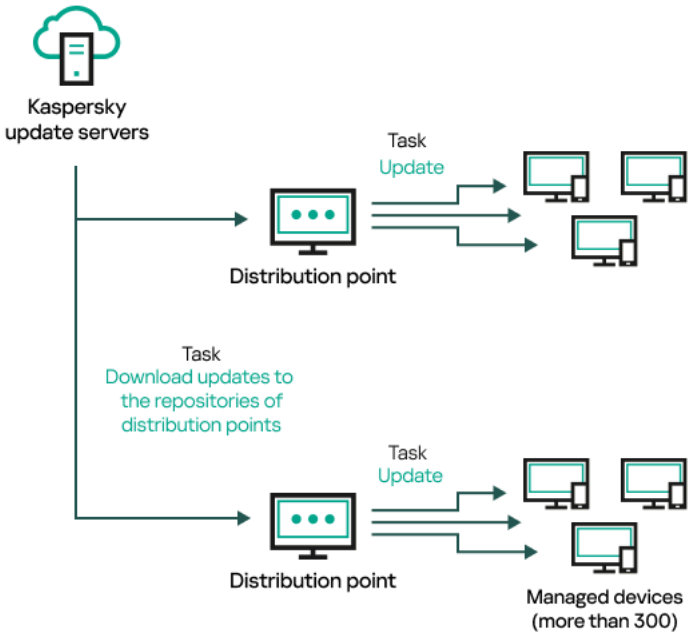
- Using the *Download updates to the repositories of distribution points* task
- Manually through a local folder, a shared folder, or an FTP server
- Directly from Kaspersky update servers to the security applications on the managed devices

Using the Download updates to the repositories of distribution points task

In this scheme, Kaspersky Next Expert View downloads updates through the *Download updates to the repositories of distribution points* task. The managed devices included in the scope of a distribution point download the updates from the repository of the distribution point (see figure below).

Distribution point devices running macOS cannot download updates from Kaspersky update servers.

If one or more devices running 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.



Updating by using the Download updates to the repositories of distribution points task

When the *Download updates to the repositories of distribution points* task is complete, the following updates are downloaded to the distribution point repository:

- Kaspersky databases and software modules for the security applications on the managed devices

  These updates are installed through the Update task for Kaspersky Endpoint Security for Windows.

- Updates for the components of Kaspersky Next Expert View

  By default, these updates are installed automatically. You can change the settings in the Network Agent policy.

- Updates for the security applications

  By default, Kaspersky Endpoint Security for Windows installs only those updates that you approve. The updates are installed through the Update task and can be configured in the properties of this task.

Each Kaspersky application requests required updates from Administration Server. Administration Server aggregates these requests and downloads to the distribution point repositories 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 repositories of distribution points* 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:

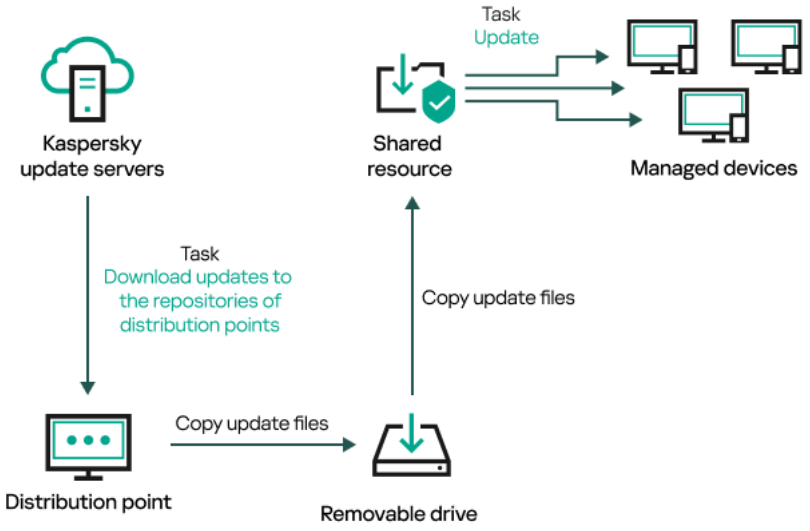
- Application ID and version
- Application setup ID

- Active key ID
- Download 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.

Through a local folder, a shared folder, or an FTP server

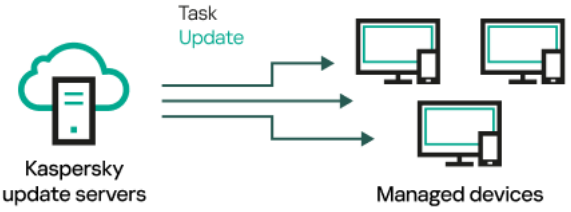
If the client devices do not have a connection to a distribution point, a local folder or a shared resource can be used as a source for updating Kaspersky databases, software modules, and applications. In this scheme, required updates are copied from a distribution point repository to a removable drive, and then the updates are copied to the local folder or the shared resource specified as an update source in the settings of Kaspersky Endpoint Security for Windows (see figure below).



Updating through a local folder, a shared folder, or an FTP server

Directly from Kaspersky update servers to Kaspersky Endpoint Security for Windows on the managed devices

On the managed devices, Kaspersky Endpoint Security for Windows receives 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 repositories provided by Kaspersky Next Expert View. To receive updates directly from Kaspersky update servers, specify Kaspersky update servers as an update source in the interface of the security application. For a full description of these settings, please refer to the Kaspersky Endpoint Security for Windows documentation.

Creating the task for downloading updates to the repositories of distribution points

Distribution point devices running macOS cannot download updates from Kaspersky update servers.

If one or more devices running 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.

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.

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 Next Expert View 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 **Asset management** → **Tasks**.
2. Click **Add**.

   The New task wizard starts. Follow the steps of the wizard.
3. For the Kaspersky Next Expert View 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 ("*<>?\:|).
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 enable the **Open task details when creation is complete** option, you can modify the default task settings. 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.
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. A network folder can be an FTP or HTTP server, or an SMB share. If a network folder requires authentication, only the SMB protocol is supported. When selecting a local folder, you must specify a folder on the device that has Administration Server installed.

    > An FTP or HTTP server or a network folder used by an update source must contain a folders structure (with updates) that matches the structure created when using Kaspersky update servers.

- **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**

  Kaspersky Next Expert View 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 13.2 or earlier version

  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 13.2 or earlier, 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**

  Select the schedule according to which the task runs, and configure the selected schedule.

  - **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.

  - **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 Monday at the current system time.

  - **Daily (daylight saving time is not supported)**

    The task runs regularly, with the specified interval in days. This schedule does not support observance of daylight saving time (DST). It means that when clocks jump one hour forward or backward at the beginning or ending of DST, the actual task start time does not change.

    We do not recommend that you use this schedule. It is needed for backward compatibility of Kaspersky Next Expert View.

    By default, the task starts every day at the current system time.

  - **Weekly**

    The task runs every week on the specified day and at the specified 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 disabled.

- **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.

- **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.

Configuring managed devices to receive updates only from distribution points

Managed devices can retrieve updates of Kaspersky databases, software modules, and Kaspersky applications from various sources: directly from update servers, from distribution points, or from a local or network folder. You can specify distribution points as the only possible source of updates.

To configure managed devices to receive updates only from distribution points:

1. In the main menu, go to **Asset management** → **Policies**.
2. Click the Network Agent policy.
3. In the policy properties window, open the **Application settings** tab.
4. In the **Settings** section, turn on the **Distribute files through distribution points only** toggle button.
5. Set the lock (🔒) for this toggle button.
6. Click the **Save** button.

The policy will be applied to the selected devices, and the devices will receive updates only from distribution points.

Enabling and disabling automatic updating and patching for Kaspersky Next Expert View components

Automatic installation of updates and patches for Kaspersky Next Expert View components is enabled by default during Network Agent installation on the device. You can disable it during Network Agent installation, or you can disable it later by using a policy.

To disable automatic updating and patching for Kaspersky Next Expert View components during local installation of Network Agent on a device:

1. Start local installation of Network Agent on the device.
2. At the **Advanced settings** step, clear the **Automatically install applicable updates and patches for components that have Undefined status** check box.
3. Follow the steps of the wizard.

Network Agent with disabled automatic updating and patching for Kaspersky Next Expert View components will be installed on the device. You can enable automatic updating and patching later by using a policy.

To disable automatic updating and patching for Kaspersky Next Expert View components during Network Agent installation on the device through an installation package:

1. In the main menu, go to **Operations** → **Repositories** → **Installation packages**.
2. Click the **Kaspersky Security Center Network Agent <version number>** package.
3. In the properties window, go to the **Settings** tab.
4. Turn off the **Automatically install applicable updates and patches for components that have the Undefined status** toggle button.

Network Agent with disabled automatic updating and patching for Kaspersky Next Expert View components will be installed from this package. You can enable automatic updating and patching later by using a policy.

If the check box in step 4 was selected (or cleared) during Network Agent installation on the device, you can subsequently enable (or disable) automatic updating by using the Network Agent policy.

To enable or disable automatic updating and patching for Kaspersky Next Expert View components by using the Network Agent policy:

1. In the main menu, go to **Asset management** → **Policies**.
2. Click the Network Agent policy.
3. In the policy properties window, select the **Application settings** tab.
4. In the **Manage patches and updates** section, turn on or off the **Automatically install applicable updates and patches for components that have the Undefined status** toggle button to enable or disable, respectively, automatic updating and patching.
5. Make sure to set (**Enforce**) the lock (🔒) for this toggle button.

The policy will be applied to the selected devices, and automatic updating and patching for Kaspersky Next Expert View components will be enabled (or disabled) on these devices.

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 **Asset management** → **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 enable the **Open task details when creation is complete** option, you can modify the default task settings. 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.
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**. The settings on this tab define how the device receives updates when connection is established between the device and the Administration Server.

    - **Mobile mode**. The settings on this tab define how the device receives updates when no connection is established between Kaspersky Next Expert View 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.

    When Kaspersky Next Expert View is set as an update source, the updates are downloaded from a distribution point repository, not from the Administration Server repository. Make sure that you have assigned distribution points and created the *Download updates to the repositories of distribution points*.

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 Next Expert View.

    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 update statuses

Status is an attribute of software updates that defines whether a particular software update must be installed on a networked device.

An update can have the following statuses:

- *Undefined*

  By default, the downloaded software updates have the *Undefined* status. The undefined updates can only be installed on Network Agent and other Kaspersky Next Expert View components in accordance with the Network Agent policy settings.

- *Approved*

  The approved updates are always installed. If an update requires reviewing and accepting the terms of the End User License Agreement, then you first need to accept the terms.

- *Declined*

  The updates for which you set *Declined* status will not be installed on devices.

You can change statuses of updates for the following software:

- Network Agent and other Kaspersky Next Expert View components

  By default, the downloaded updates and patches for Kaspersky Next Expert View components are installed automatically. If you have left the **Automatically install applicable updates and patches for components that have the Undefined status** option enabled in the Network Agent properties, then all updates will be installed automatically after they are downloaded to the repository (or several repositories). 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*.

  Updates for Kaspersky Next Expert View components cannot be uninstalled, even if you set an update the *Declined* status.

- Kaspersky security applications

  By default, updates for the managed applications are installed only after you change the update status to *Approved*. If a declined update for a security application was previously installed, Kaspersky Next Expert View will try to uninstall the update from all devices.

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 and Linux-based client devices. Seamless updating of Administration Server, Kaspersky Next Expert View, 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 **Operations** → **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.

   To view the data processed by Kaspersky applications for which you want to approve seamless updates, click **View the list of data** in the opened License Agreement pane.

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 Next Expert View 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.

Using diff files for updating Kaspersky 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 limits traffic on 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 a distribution point, the diff files are saved on this distribution point. As a result, devices that take updates from this 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 distribution point from which the devices take updates. However, the traffic can be saved even if devices are updated several times less often than is the distribution point from which the devices take updates.

Distribution points do not use IP multicasting for automatic distribution of diff files.

To enable the Downloading diff files feature:

1. In the main menu, go to **Asset management** → **Tasks**.
2. Click the *Download updates to the repositories of distribution points* task to open the task properties.
3. On the **Application settings** tab, enable the **Download diff files** option.
4. Click the **Save** button.

   The Downloading diff files feature is enabled. Diff files of updates will be downloaded in addition to the update files each time the *Download updates to the repositories of distribution points* task is run.

To check that the Downloading diff files feature is successfully enabled, you can measure the internal traffic before and after you perform the scenario.

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 repositories of distribution points.

When you need to update databases and software modules on a device (or a group of devices) that is not connected to 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 following sources:

- Distribution point.

  To be sure the distribution point repository contains the updates required for the security application installed on an offline device, at least one of the managed online devices in the scope of the distribution point must have the same security application installed. This application must be configured to receive the updates from the distribution point repository through the *Download updates to the repositories of distribution points* task.

- Any device that has the same security application installed and configured to receive the updates from 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 a distribution point repository.

To update Kaspersky databases and software modules on offline devices:

1. Connect the removable drive to the distribution point device.

2. Copy the updates files to the removable drive.

   By default, the updates are located at: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates.

3. On offline devices, configure the security application (for example, Kaspersky Endpoint Security for Windows) to receive updates from a local folder or a shared resource, such as an FTP server or a shared folder.

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 Windows.

   After the update task is complete, the Kaspersky databases and software modules are up-to-date on the device.

Managing third-party applications on client devices

This section describes the features of Kaspersky Next Expert View that are related to the management of third-party applications installed on client devices.

Limitations of Vulnerability and patch management

The Vulnerability and patch management feature has a number of limitations, depending on the license that you use and the mode in which Kaspersky Next Expert View is working.

The following licenses do not support Vulnerability and patch management:

- Kaspersky Endpoint Security for Business Select
- Kaspersky Hybrid Cloud Security

The following licenses support Vulnerability and patch management:

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Total Security for Business
- Kaspersky Hybrid Cloud Security Enterprise

The table below compares limitations of Kaspersky Next Expert View in the trial mode, under licenses that do not support Vulnerability and patch management, and under licenses that support Vulnerability and patch management.

Limitations of Vulnerability and patch management

Limitation	Trial mode	Commercial mode: licenses that do not support Vulnerability and patch management	Commercial mode: licenses that support Vulnerability and patch management
Maximum number of the *Install Windows Update updates* tasks or the *Fix vulnerabilities* tasks	4	4	0 (new tasks of these types cannot be created)
Maximum number of the *Install required updates and fix vulnerabilities* tasks	2	Not supported	4
Maximum number of rules in all of the *Install required updates and fix vulnerabilities* tasks	10	Not supported	50
Maximum number of software updates that can have the *Approved* status at the same time, across all servers including virtual ones	100	Not supported	1000
Maximum number of software updates that can be manually added to a task, across all servers including virtual ones	500	1000	1000
Maximum number of software vulnerabilities that can be manually added to a task, across all servers including virtual ones	500	1000	1000

Availability of Vulnerability and patch management features in trial and commercial mode and under various licensing options

The availability of Vulnerability and patch management features in Kaspersky Next Expert View depends on whether you use it in trial or commercial mode, as well as on the licensing option that you selected. Use the table to check which Vulnerability and patch management features are available.

Availability of Vulnerability and patch management features

Vulnerability and patch management	Trial mode	Commercial mode: Kaspersky Endpoint Security for Business Select	Commercial mode: Kaspersky Endpoint Security for Business Advanced, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Total Security for Business
Manual fixing of vulnerabilities in Microsoft software on managed devices that are running Windows Creating the *Fix vulnerabilities* task	✓	✓	–
Manual installation of updates in Microsoft software on managed devices that are running Windows Installing third-party software updates through the *Install Windows Update updates* task	–	✓	✓
Automatic rule-based installing third-party software updates and fixing of third-party software vulnerabilities Creating the *Install required updates and fix vulnerabilities* task and installing updates Adding rules for update installation	✓	–	✓

About third-party applications

Kaspersky Next Expert View can help you to update third-party software, installed on client devices, and fix the vulnerabilities of the third-party software. Kaspersky Next Expert View 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 Next Expert View by viewing the list of available updates in Kaspersky Next Expert View.

The procedure outlined below is intended solely for viewing the list of third-party software that can be updated with Kaspersky Next Expert View. 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 Next Expert View:

1. In the main menu, go to **Asset management** → **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 Next Expert View**.
   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.

Third-party software updates

Kaspersky Next Expert View enables you to manage updates of third-party software installed on managed devices and fix vulnerabilities in Microsoft applications and other software makers' products through installation of required updates.

Kaspersky Next Expert View 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 devices.

Kaspersky Next Expert View 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.

Tasks for installation of third party software updates

When metadata of the third-party software updates is downloaded to the repository, you can install the updates on client devices by using the following tasks:

- The *Install required updates and fix vulnerabilities* task

  This task is used to install updates for Microsoft applications, including the updates provided by the Windows Update service, and updates of other vendors' software.

  When this task is complete, the updates are installed on the managed devices automatically. When metadata of new updates is downloaded to the Administration Server repository, Kaspersky Next Expert View 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.

- The *Install Windows Update updates* task

  This task can be used to install Windows Update updates only.

  When this task is complete, only those updates that are specified in the task properties are installed. In future, if you want to install new updates, you must add the required updates to the list of updates in the existing task or create an *Install Windows Update updates* task.

The software update installation tasks have a number of limitations. These limitations depend on the license under which you are using Kaspersky Next Expert View and on the mode in which Kaspersky Next Expert View is working.

Scenario: Updating third-party software

This section provides a scenario for updating third-party software installed on client devices. The third-party software includes applications from Microsoft and other software vendors. Updates for Microsoft applications are provided by the Windows Update service.

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 Next Expert View 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 task or run the quick start wizard now.

   How-to instructions:

   - Creating the Find vulnerabilities and required updates task
   - Find vulnerabilities and required updates task settings

2. **Analyzing the list of found updates**

   View the **Software updates** list 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 view the statistics about the update installation on managed devices. For example, you can view the number of devices on which the selected update is not installed, will be installed, or on which the update installation has failed.

   How-to instructions: Viewing information about available third-party software updates

3. **Configuring installation of updates**

   When Kaspersky Next Expert View received the list of the third-party software updates, you can install them on client devices by using the *Install required updates and fix vulnerabilities* task or the *Install Windows Update updates* task. Create one of these tasks. You can create these tasks on the **Tasks** tab or by using the **Software updates** list.

   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.

   The *Install Windows Update updates* task can be used to install Windows Update updates only.

   The software update installation tasks have a number of limitations. These limitations depend on the license under which you are using Kaspersky Next Expert View and on the mode in which Kaspersky Next Expert View is working.

   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.

How-to instructions:

- Creating the Install required updates and fix vulnerabilities task
- Creating the Install Windows Update updates task
- Viewing information about available third-party software updates

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. The default 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 *Install Windows Update updates* task, note that for this task you must define the list of updates every time before starting this task.

   When scheduling the tasks, make sure that a task to fix vulnerability starts after the *Find vulnerabilities and required updates* task is complete.

   How-to instructions: General task settings

5. **Approving and declining software updates (optional)**

   If you have created the *Install required updates and fix vulnerabilities* task, you can specify rules for update installation in the task properties. If you have created the *Install Windows Update updates* task, skip this step.

   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 Windows Update updates and only those ones that have *Approved* status. After that you manually set the *Approved* status for those updates that you want to install. In this case the Windows Update updates that have the *Undefined* or *Declined* status will not be installed on the servers that you specified in the task.

   By default, the downloaded software updates have the *Undefined* status. You can change the status to *Approved* or *Declined* in the **Software updates** list (**Operations** → **Patch management** → **Software updates**).

   How-to instructions: Approving and declining third-party software updates

6. **Running an update installation task**

   Start the *Install required updates and fix vulnerabilities* task or the *Install Windows Update updates* task. When you start these tasks, 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.

   How-to instructions: Starting a task manually

7. **Create the report on results of update installation of third-party software (optional)**

   To verify that the task has been created and the updates have been installed, create a **Report on results of installation of third-party software updates**, in which you can view detailed statistics of the installation of updates.

   How-to instructions: Generating and viewing a report

Installing third-party software updates

You can install third-party software updates on managed devices by creating and running one of the following tasks:

- *Install required updates and fix vulnerabilities*

  You can use this task to install both Windows Update updates provided by Microsoft and updates of other vendors' software.

- *Install Windows Update updates*

  You can use this task to install Windows Update updates only.

The software update installation tasks have a number of limitations. These limitations depend on the license under which you are using Kaspersky Next Expert View and on the mode in which Kaspersky Next Expert View is working.

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 availability of the Update installation wizard depends on the Kaspersky Next Expert View mode and your current 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 one of the lists of updates:

   - To open the general update list, in the main menu, go to **Operations** → **Patch management** → **Software updates**.
   - To open the list of updates for a managed device, in the main menu, go to **Asset management** → **Assets (Devices)** → **<device name>** → **Advanced** → **Available updates**.
   - To open the list of updates for a specific application, in the main menu, go to **Operations** → **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.

   To install some software updates, you must accept the End User License Agreement (EULA). If you decline the EULA, the software update will not be installed.

4. Choose one of the following options:

   - **New task**

     The New task wizard starts. The *Install required updates and fix vulnerabilities* task or the *Install Windows Update updates* task is preselected, depending on the Kaspersky Next Expert View mode and your current license. 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. Select an *Install required updates and fix vulnerabilities* task or an *Install Windows Update updates* task. If you select an *Install required updates and fix vulnerabilities* task, a new rule to install the selected updates will be automatically added to the selected task. If you select an *Install Windows Update updates* task, the selected updates will be 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 **Asset management** → **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, start the *Install required updates and fix vulnerabilities* task or the *Install Windows Update updates* task. You can start any of these tasks manually or specify 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 availability of this feature depends on the Kaspersky Next Expert View mode and your current license.

To create a task to install third-party software updates by using the Update installation wizard:

1. In the main menu, go to **Operations** → **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*
   - *Install Windows Update updates*
   - *Fix vulnerabilities*

   You cannot modify the tasks of the last two types to install new updates. To install new updates, you can only use the *Install required updates and fix vulnerabilities* tasks.

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 a task, select the check box next to the task name, and then click the **Start** button.
   - 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.

     b. On the page that opens, 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.

     - **Installation rule for updates of this importance level according to MSRC** (available only for Windows Update updates)

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.

- **Installation rule for updates by this vendor** (available only for updates of third-party applications)

  This option is available only for updates of third-party applications. Kaspersky Next Expert View 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.

- **Installation rule for updates of the type**

- **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**.

- To create a task:

  a. Click the **New task** button.

  b. On the page that opens, 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.

- **Installation rule for updates of this importance level according to MSRC** (available only for Windows Update updates)

  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.

- **Installation rule for updates by this vendor** (available only for updates of third-party applications)

  This option is available only for updates of third-party applications. Kaspersky Next Expert View 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.

- **Installation rule for updates of the type**

- **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**.

If you have chosen to start a task, you can close the wizard. The task will complete in background mode. No further actions are required.

If you have chosen to add a rule to an existing task, 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.

If you have chosen to create a task, you 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 New task wizard, the *Install required updates and fix vulnerabilities* task is added to the task list.

Creating the Find vulnerabilities and required updates task

Through the Find vulnerabilities and required updates task, Kaspersky Next Expert View receives the lists of detected vulnerabilities and required updates for the third-party software installed on the managed devices.

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 **Asset management** → **Tasks**.
2. Click **Add**.

   The New task wizard starts. Follow the steps of the wizard.
3. For the Kaspersky Next Expert View 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. 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.
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. In the task properties window, specify the general task settings.

10. On the **Application settings** tab, specify the following settings:

- **Search for vulnerabilities and updates listed by Microsoft**

  When searching for vulnerabilities and updates, Kaspersky Next Expert View 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:

  - Kaspersky Next Expert View Administration Server (see the settings of Network Agent policy)
  - 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 **Disabled** option is set to **Windows Update search mode**, Kaspersky Next Expert View does not request any information about updates.

- **Search for third-party vulnerabilities and updates listed by Kaspersky**

  If this option is enabled, Kaspersky Next Expert View 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 Next Expert View 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 Next Expert View 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 is empty.

- **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 Next Expert View 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 Next Expert View 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.

11. Click the **Save** button.

The task is created and configured.

If the task results contain a warning of the 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" error, you can resolve this issue through the Windows Registry.

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 Next Expert View 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:

  - Kaspersky Next Expert View Administration Server (see the settings of Network Agent policy)
  - 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 **Disabled** option is set to **Windows Update search mode**, Kaspersky Next Expert View does not request any information about updates.

- **Search for third-party vulnerabilities and updates listed by Kaspersky**

  If this option is enabled, Kaspersky Next Expert View 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 Next Expert View 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 Next Expert View 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 is empty.

- **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 Next Expert View 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 Next Expert View 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 Install required updates and fix vulnerabilities task

The availability of the *Install required updates and fix vulnerabilities* task depends on the Kaspersky Next Expert View mode and your current license.

The *Install required updates and fix vulnerabilities* task is used to update and fix vulnerabilities in third-party software, including Microsoft software, installed on the managed devices. This task enables you to install multiple updates and fix multiple vulnerabilities according to certain rules.

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.

The software update installation tasks have a number of limitations. These limitations depend on the license under which you are using Kaspersky Next Expert View and on the mode in which Kaspersky Next Expert View is working.

To create the Install required updates and fix vulnerabilities task:

1. In the main menu, go to **Asset management** → **Tasks**.
2. Click **Add**.

   The New task wizard starts. Follow the steps of the wizard.
3. For the Kaspersky Next Expert View application, select the **Install required updates and fix vulnerabilities** 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 rules for update installation, and then specify the following settings:

   - **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 Next Expert View 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 Next Expert View 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.

7. 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.

8. If you want to modify the default task settings, enable the **Finish task creation** option on the **Open task details when creation is complete** 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.

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.

12. Click the **Save** button.

    The task is created and configured.

If the task results contain a warning of the 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" error, you can resolve this issue through the Windows Registry.

Adding rules for update installation

The availability of this feature depends on the Kaspersky Next Expert View mode and your current 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 specific updates that you want to install and vulnerabilities that you want to fix by means of 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 properties window of an existing *Install required updates and fix vulnerabilities* task.
- Through the Update installation wizard or the Vulnerability fix wizard.

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. On the **Rule type** page, select **Rule for all updates**.

3. On the **General criteria** page, use the drop-down lists to 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.

4. On the **Updates** page, select the updates to be installed:

   - **Install all suitable updates**

     Install all software updates that meet the criteria specified on the **General criteria** page 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.

5. On the **Vulnerabilities** page, select 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 on the **General criteria** page 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.

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.

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. On the **Rule type** page, select **Rule for Windows Update**.

3. On the **General criteria** page, 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.

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. On the **Rule type** page, select **Rule for third-party updates**.

3. On the **General criteria** page, 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.

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 **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.

Creating the Install Windows Update updates task

The Install Windows Update updates task enables you to install software updates provided by the Windows Update service on client devices.

The software update installation tasks have a number of limitations. These limitations depend on the license under which you are using Kaspersky Next Expert View and on the mode in which Kaspersky Next Expert View is working.

To create the Install Windows Update updates task:

1. In the main menu, go to **Asset management** → **Tasks**.

2. Click **Add**.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.

3. For the Kaspersky Next Expert View application, select the **Install Windows Update updates** task type.

4. 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 ("*<>?\:|).

5. Select the devices to which the task will be assigned.

6. Click **Add**.

   The list of updates opens.

7. Select the Windows Update updates that you want to install, and then click **OK**.

8. 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.

9. 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.

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 task is created and displayed in the list of tasks.

12. Click the name of the created task to open the task properties window.

13. In the task properties window, specify the general task settings according to your needs.

14. Click the **Save** button.

The task is created and configured.

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 **Operations** → **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 ( ) in the upper right corner 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)
  - Windows Server Update Services (WSUS) category to which the update belongs
  - 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 on which the update has 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** → **Assets (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, that is displayed at the moment to the CSV or TXT files. 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**.

   The page displays a list of available updates for third-party software installed on all managed devices.

2. Click the **Export to TXT** or **Export to CSV** button, depending on the format you prefer for export.

The file containing the list of available updates for third-party software, including Microsoft software, is downloaded to the device that you use at the moment.

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.

2. Select the software updates you want to export.

   Skip this step if you want to export a complete list of software updates.

   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 installed updates, select the **Show installed updates** check box.

3. Click the **Export to TXT** or **Export to CSV** button, depending on the format you prefer for export.

The file containing the list of updates for third-party software, including Microsoft software, installed on the selected managed device is downloaded to the device you are using at the moment.

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 *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 amount of updates, performance of Administration Server decreases and may lead to Administration Server overload.

To approve or decline one or several updates:

1. In the main menu, go to **Operations → Patch management → Software updates**.

   A list of available updates appears.

2. Select the updates that you want to approve or decline.

3. Click **Approve** to approve the selected updates or **Decline** to decline the selected updates.

   The default value 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 **Operations → 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 by changing the **Update approval status** option. 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 **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 them, you can manually delete them locally.

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*, *Install Windows Update updates*, and *Fix vulnerabilities*.

To configure the auto-update setting for a third-party application:

1. In the main menu, go to **Operations → Third-party applications → Applications registry**.

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** column.

   The application properties window opens.

3. In the **General** section, select a value for the following setting:

   Automatic Updates status

Choose one of the following options:

- **Undefined**

  The auto-update feature is disabled. Kaspersky Next Expert View installs third-party application updates by using the tasks: *Install required updates and fix vulnerabilities*, *Install Windows Update updates*, 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 Next Expert View installs third-party application updates by using the tasks: *Install required updates and fix vulnerabilities*, *Install Windows Update updates*, and *Fix vulnerabilities*.

4. Click **Save** to save the changes.

The auto-update setting is applied to the selected application.

Finding and fixing software vulnerabilities

Kaspersky Next Expert View detects and fixes software vulnerabilities on managed devices running Microsoft Windows families 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 Next Expert View uses characteristics from the database of known vulnerabilities and Windows Update Database. The database of known vulnerabilities is created and maintained by Kaspersky specialists. It contains information about vulnerabilities, such as vulnerability description, vulnerability detect date, vulnerability severity level. You can find the details of software vulnerabilities on Kaspersky website.

Kaspersky Next Expert View uses the *Find vulnerabilities and required updates* task to find software vulnerabilities.

Fixing software vulnerabilities

To fix software vulnerabilities, Kaspersky Next Expert View uses software updates issued by the software vendors. You can view the list of software vulnerabilities at any time. The software updates metadata is downloaded to the Administration Server repository automatically and to the repositories of distribution points as a result of the *Download updates to the repositories of distribution points* task run. You can create this task by the Kaspersky Next Expert View quick start wizard or manually.

Software updates to fix vulnerabilities can be represented as full distribution packages or patches. Software updates that fix software vulnerabilities are named *fixes*. In Kaspersky Next Expert View, you fix vulnerabilities by using *recommended fixes*. Recommended fixes are software updates that are recommended for installation by Kaspersky specialists.

Depending on the Kaspersky Next Expert View mode and your current license, you can use *Install required updates and fix vulnerabilities* task or the *Fix vulnerabilities* task to fix software vulnerabilities.

The *Install required updates and fix vulnerabilities* task automatically fixes multiple vulnerabilities installing recommended fixes. For this task, you can manually configure certain rules to fix multiple vulnerabilities.

By means of the *Fix vulnerabilities* task, you can fix vulnerabilities by installing recommended fixes for Microsoft 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.

The software update installation tasks have a number of limitations. These limitations depend on the license under which you are using Kaspersky Next Expert View and on the mode in which Kaspersky Next Expert View is working.

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 EULA, the software vulnerability cannot be fixed.

The information about each fixed vulnerability is stored on the Administration Server for 90 days. After this time, it is automatically deleted.

Fixing software vulnerabilities

After you obtain the software vulnerabilities list, you can fix software vulnerabilities on 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.

The software update installation tasks have a number of limitations. These limitations depend on the license under which you are using Kaspersky Next Expert View and on the mode in which Kaspersky Next Expert View is working.

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 availability of this feature depends on the Kaspersky Next Expert View mode and your current license.

  The wizard simplifies creation and configuration of a vulnerability fix task and enables you to eliminate the creation of redundant tasks that contain the same updates to install.

Fixing software vulnerabilities by using the vulnerability list

To fix software vulnerabilities:

1. Open one of the lists of vulnerabilities:

   - To open the general vulnerability list, in the main menu, go to **Operations** → **Patch management** → **Software vulnerabilities**.
   - To open the vulnerability list for a managed device, in the main menu, go to **Asset management** → **Assets (Devices)** → **device name** → **Advanced** → **Software vulnerabilities**.
   - To open the vulnerability list for a specific application, in the main menu, go to **Operations** → **Third-party applications** → **Applications registry** → **application name** → **Vulnerabilities**.

   A page with a list of vulnerabilities in the third-party software is displayed.

2. Select one or more vulnerabilities in the list, 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. Depending on the Kaspersky Next Expert View mode and your current license, the *Install required updates and fix vulnerabilities* task or 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. Depending on the Kaspersky Next Expert View mode and your current license, select an *Install required updates and fix vulnerabilities* task or a *Fix vulnerabilities* task. If you select an *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 select a *Fix vulnerabilities* task, the selected vulnerabilities will be 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 **Asset management** → **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 to fix the software vulnerabilities listed in the task settings.

Fixing software vulnerabilities by using the Vulnerability fix wizard

The availability of the Vulnerability fix wizard depends on the license that you use and the mode in which Kaspersky Next Expert View is working.

To fix software vulnerabilities by using the Vulnerability fix wizard:

1. In the main menu, go to **Operations** → **Patch management** → **Software vulnerabilities**.

   A table with the 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 Vulnerability fix wizard starts. The **Select the vulnerability fix task** page displays the list of all existing tasks of the following types:

   - *Install required updates and fix vulnerabilities*
   - *Install Windows Update updates*
   - *Fix vulnerabilities*

   You cannot modify the last two types of tasks 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. Choose what you want to do:

- To start a task, select the check box next to the task name, and then click the **Start** button.
- 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.

  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** (available only for Microsoft software vulnerabilities)
  - **Rule for fixing vulnerabilities in applications from the selected vendor** (available only for third-party software vulnerabilities)
  - **Rule for fixing a vulnerability in all versions of the selected application** (available 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**.

- 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 using updates of the type** (available only for Microsoft software vulnerabilities)
- **Rule for fixing vulnerabilities in applications from the selected vendor** (available only for third-party software vulnerabilities)
- **Rule for fixing a vulnerability in all versions of the selected application** (available 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**.

If you have chosen to start a task, you can close the wizard. The task will complete in background mode. No further actions are required.

If you have chosen to add a rule to an existing task, 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.

If you have chosen to create a task, you continue to create the task in the New task wizard. The new rule that you added in the Vulnerability fix wizard is displayed in the New task wizard. When you complete the New task wizard, the *Install required updates and fix vulnerabilities* task is added to the task list.

Creating the Fix vulnerabilities task

The *Fix vulnerabilities* task enables you fix vulnerabilities in Microsoft software on managed devices that are running Windows.

The availability of this feature depends on the Kaspersky Next Expert View mode and your current license. 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.

The software update installation tasks have a number of limitations. These limitations depend on the license under which you are using Kaspersky Next Expert View and on the mode in which Kaspersky Next Expert View is working.

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 **Asset management** → **Tasks**.
2. Click **Add**.

   The New task wizard starts. Proceed through the wizard by using the **Next** button.
3. For the Kaspersky Next Expert View application, select the **Fix vulnerabilities** task type.
4. 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 ("*<>?\:|).
5. Select the devices to which the task will be assigned.
6. Click **Add**.

   The list of vulnerabilities opens.
7. Select the vulnerabilities that you want to fix, and then click **OK**.
8. 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.

9. 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.

10. If you want to modify the default task settings, enable the **Finish task creation** option on the **Open task details when creation is complete** 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 task is created and displayed in the list of tasks.

12. Click the name of the created task to open the task properties window.

13. In the task properties window, specify the general task settings according to your needs.

14. Click the **Save** button.

The task is created and configured.

Creating the Install required updates and fix vulnerabilities task

The availability of the *Install required updates and fix vulnerabilities* task depends on the Kaspersky Next Expert View mode and your current license.

The *Install required updates and fix vulnerabilities* task is used to update and fix vulnerabilities in third-party software, including Microsoft software, installed on the managed devices. This task enables you to install multiple updates and fix multiple vulnerabilities according to certain rules.

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.

The software update installation tasks have a number of limitations. These limitations depend on the license under which you are using Kaspersky Next Expert View and on the mode in which Kaspersky Next Expert View is working.

To create the Install required updates and fix vulnerabilities task:

1. In the main menu, go to **Asset management** → **Tasks**.
2. Click **Add**.

   The New task wizard starts. Follow the steps of the wizard.
3. For the Kaspersky Next Expert View application, select the **Install required updates and fix vulnerabilities** 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 rules for update installation, and then specify the following settings:

   - **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 Next Expert View 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 Next Expert View 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.

7. 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.

8. If you want to modify the default task settings, enable the **Finish task creation** option on the **Open task details when creation is complete** 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.

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.

12. Click the **Save** button.

    The task is created and configured.

If the task results contain a warning of the 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")" error, you can resolve this issue through the Windows Registry.

Adding rules for update installation

The availability of this feature depends on the Kaspersky Next Expert View mode and your current 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 specific updates that you want to install and vulnerabilities that you want to fix by means of 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 properties window of an existing *Install required updates and fix vulnerabilities* task.
- Through the Update installation wizard or the Vulnerability fix wizard.

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. On the **Rule type** page, select **Rule for all updates**.

3. On the **General criteria** page, use the drop-down lists to 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.

4. On the **Updates** page, select the updates to be installed:

- **Install all suitable updates**

  Install all software updates that meet the criteria specified on the **General criteria** page 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.

5. On the **Vulnerabilities** page, select 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 on the **General criteria** page 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.

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.

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. On the **Rule type** page, select **Rule for Windows Update**.

3. On the **General criteria** page, 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.

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. On the **Rule type** page, select **Rule for third-party updates**.

3. On the **General criteria** page, 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.

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 **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.

Viewing information about software vulnerabilities detected on all managed devices

After you have scanned software on managed devices for vulnerabilities, you can view the list of software vulnerabilities detected on all managed devices. 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.

To view the list of software vulnerabilities detected on all managed devices,

In the main menu, go to **Operations** → **Patch management** → **Software vulnerabilities**.

The page displays the list of software vulnerabilities detected on client devices.

You can also generate and view a Report on vulnerabilities.

You can specify a filter to view the list of software vulnerabilities. Click the **Filter** icon () in the upper right corner of the software vulnerabilities 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.

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** → **Assets (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.

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 export the displayed list of vulnerabilities to the CSV or TXT files. You can use these files, for example, to send to your information security manager or to store them for statistical purposes.

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**.

   The page displays a list of vulnerabilities for the applications detected on managed devices.

2. Click the **Export to TXT** or **Export to CSV** button, depending on the format you prefer for export.

The file containing the list of software vulnerabilities is downloaded to the device that you use at the moment.

To export the list of software vulnerabilities detected on selected managed device to a text file:

1. Open the list of software vulnerabilities detected on selected managed device.

2. Select the software vulnerabilities you want to export.

   Skip this step if you want to export a complete list of software vulnerabilities detected on the managed device.

   If you want to export complete list of software vulnerabilities detected on the managed device, only vulnerabilities displaying on the current page will be exported.

3. Click the **Export to TXT** or **Export to CSV** button, depending on the format you prefer for export.

The file containing the list of software vulnerabilities detected on the selected managed device is downloaded to the device you are using at the moment.

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**.

   The page displays the list of software vulnerabilities detected on managed devices.

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** setting.

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** → **Assets (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.

Scenario: Finding and fixing 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 Next Expert View is deployed in your organization.
- There are managed devices running Windows in your organization.

Stages

Finding and fixing software vulnerabilities proceeds in stages:

1. **Scanning for vulnerabilities in the software installed on the client devices**

   To find vulnerabilities in the software installed on the managed devices, run the *Find vulnerabilities and required updates* task. When this task is complete, Kaspersky Next Expert View 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 Kaspersky Next Expert View quick start wizard. If you did not run the wizard, start it now or create the task manually.

   How-to instructions: Creating the Find vulnerabilities and required updates task

2. **Analyzing the list of detected software vulnerabilities**

   View the **Software vulnerabilities** list and decide which vulnerabilities are 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.

   How-to instructions:

   - Viewing information about software vulnerabilities
   - Viewing statistics of vulnerabilities on managed devices

3. **Configuring vulnerabilities fix**

   When the software vulnerabilities are detected, you can fix the software vulnerabilities on the 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 the managed devices. This task enables you to install multiple updates and fix multiple vulnerabilities according to certain rules. Availability of this task depends on the Kaspersky Next Expert View mode and your current license. To fix software vulnerabilities, the *Install required updates and fix vulnerabilities* task uses recommended software updates.

   The *Fix vulnerabilities* task uses recommended fixes for Microsoft software.

   You can start Vulnerability fix wizard that creates one of these tasks automatically, or you can create one of these tasks manually.

   How-to instructions: Fixing vulnerabilities in third-party software, Creating the Install required updates and fix vulnerabilities

4. **Scheduling the tasks**

   To be sure that the vulnerabilities list is always up-to-date, schedule the *Find vulnerabilities and required updates* task to run it automatically from time to time. The recommended average 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 every time before starting the task.

When scheduling the tasks, make sure that a task to fix vulnerability starts after the *Find vulnerabilities and required updates* task is complete.

5. **Ignoring software vulnerabilities (optional)**

   If you want, you can ignore software vulnerabilities to be fixed on all managed devices or only on the selected managed devices.

   How-to instructions: Ignoring software vulnerabilities

6. **Running a vulnerability fix task**

   Start the *Install required updates and fix vulnerabilities* task or the *Fix vulnerabilities* task. After 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 fix, generate the Report on vulnerabilities. The report displays information about software vulnerabilities that are not fixed. Thus you can have an idea about finding and fixing vulnerabilities in third-party software, including Microsoft software, in your organization.

   How-to instructions: Generating and viewing a report

8. **Checking configuration of finding and fixing vulnerabilities in third-party software**

   Make sure of the following:

   - The list of software vulnerabilities on managed devices is not empty.
   - A task to fix vulnerabilities is in the task list.
   - The tasks to find and to fix software vulnerabilities are scheduled so that they start sequentially. View the properties of these tasks and compare their schedule.
   - The task to fix software vulnerabilities was successfully completed. View information on the **Results** tab of the task properties window.

Results

If you have created and configured the *Install required updates and fix vulnerabilities* task, the vulnerabilities are fixed on managed devices automatically. When the task is run, 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 rules will be downloaded to the repositories of distribution points and will be installed to fix software vulnerabilities, except for Windows Updates. To install Windows Updates, you have to ensure the access to Microsoft Updates public servers on your managed devices.

If you have created the *Fix vulnerabilities* task, only software vulnerabilities in Microsoft software are fixed.

Setting the maximum storage period for the information about fixed vulnerabilities

To set the maximum storage period in the database for the information about the vulnerabilities that have already been fixed on managed devices:

1. In the main menu, click the Administration Server name.

   The Administration Server properties window opens.

2. On the page that opens, proceed to the **Events repository** tab.

3. Specify the maximum storage period for the information about the fixed vulnerabilities in the database.

   By default, the storage period is 7 days in the trial mode and 60 days in the commercial mode. The maximum limit is 14 days in the trial mode and 365 days in the commercial mode.

4. Click the **Save** button.

The maximum storage period for the information about the fixed vulnerabilities is limited to the specified number of days.

Managing applications run on client devices

This section describes the features of Kaspersky Next Expert View related to the management of applications 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 Next Expert View is deployed in your organization.
- The policy of Kaspersky Endpoint Security for Windows or Kaspersky Endpoint Security for Linux is created and is active.

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 installed 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.

   How-to instructions: Creating application category with content added manually, Creating application category that includes executable files from selected devices

3. **Configuring Application Control in the Kaspersky Endpoint Security for Windows policy**

   Configure the Application Control component in Kaspersky Endpoint Security for Windows 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: Configuring Application Control component in the Kaspersky Endpoint Security for Windows policy. Follow this instruction and enable the test mode in configuration process.

5. **Changing the categories 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 an application category with content added manually.

   How-to instructions: 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: Configuring Application Control component in the Kaspersky Endpoint Security for Windows policy. Follow this instruction and disable the test mode in configuration process.

7 **Verifying Application Control configuration**

Make sure of the following:

- The list of categories for executable files is not empty. View the list of categories and make sure it contains the categories you have configured.
- Application Control is configured using created categories for executable files. View the settings of the Kaspersky Endpoint Security for Windows policy and make sure you have configured Application Control in the **Application settings** → **Security Controls** → **Application Control**.
- The rules of Application Control are applied in operation mode. Check the mode in the Kaspersky Endpoint Security for Windows policy and make sure you have disabled the **Test mode** in the **Application settings** → **Security Controls** → **Application Control**.

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 following Help topics:

- Kaspersky Endpoint Security for Windows Help
- Kaspersky Endpoint Security for Linux Help

Application Control modes and categories

The Application Control component monitors users' attempts to start executable files. You can use Application Control rules to control the startup of executable files.

> Application Control component is available for Kaspersky Endpoint Security for Windows and for Kaspersky Endpoint Security for Linux (version 11.2 and later). All the instructions in this section describe configuration of Application Control for Kaspersky Endpoint Security.

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. By default, the *Denylist* mode is selected.
- *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 Next Expert View there are two types of categories:

- Category with content added manually. You define conditions, for example, file metadata, file hashcode, file certificate, KL category, 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.

For detailed information about Application Control, refer to the following Help topics:

- Kaspersky Endpoint Security for Windows Help
- Kaspersky Endpoint Security for Linux Help

Obtaining and viewing a list of applications installed on client devices

Kaspersky Next Expert View 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 **Operations** → **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, list of available software updates, and list of detected software vulnerabilities.

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 **Table 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** → **Assets (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 following Help topics:

- Kaspersky Endpoint Security for Windows Help
- Kaspersky Endpoint Security for Linux Help

Obtaining and viewing a list of executable files installed 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

The feature of inventorying executable files is available for the following applications:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux (version 11.2 and later)

You can reduce load on the database while obtaining information about the installed applications. To do this, we recommend that you 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 **Asset management** → **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, in the **Application** drop-down list, select Kaspersky Endpoint Security for Windows or Kaspersky Endpoint Security for Linux, depending on the operating system type 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 is complete, 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, refer to the following Helps:

- Kaspersky Endpoint Security for Windows Help
- Kaspersky Endpoint Security for Linux Help

After the **Inventory** task is performed, the list of executable files installed 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 **Operations** → **Third-party applications** → **Executable files**.

The page displays the list of executable files installed on client devices.

If necessary, you can send the executable file of the managed device to the device where your Kaspersky Next Expert View is open.

To send an executable file:

1. In the main menu, go to **Operations** → **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. To do it, you can either use a distribution point as a push server with the default port (13295) or select the **Do not disconnect from the Administration Server** check box. The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

4. Click the **Send** button.

The selected executable file is downloaded for further sending to the device where your Kaspersky Next Expert View 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 **Operations** → **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, 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 category from the list:

   - **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 file or folder on the client device containing the executable files that are to be added to the user application category. You can use regular expressions such as *C:\path_to_exe**, for example: *C:\Program Files\Internet Explorer**.

- **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 must select an algorithm for hash value computing by Kaspersky Next Expert View 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 10 Service Pack 2 for Windows and later versions support SHA256 computing. Computing of the MD5 hash function is supported by all versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Select either of the options of hash value computing by Kaspersky Next Expert View for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions, select the **SHA256** check box. We do not recommend that you add any categories created according to the criterion of the SHA256 hash of an executable file for versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows. This may result in failures in the security application operation. In this case, you can use the MD5 cryptographic hash function for files of the category.

- If any versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows are installed on your network, select the **MD5 hash**. You cannot add a category that was created based on the criterion of the MD5 checksum of an executable file for Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions. In this case, you can use the SHA256 cryptographic hash function for files of the category.

- If different devices on your network use both earlier and later versions of Kaspersky Endpoint Security 10, select both the **SHA256** check box and the **MD5 hash** check box.

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 file or from MSI package/archived folder**

  If this option is selected, you can specify an MSI installer file as the condition of adding applications to the user category. The application installer metadata will be sent to Administration Server. The applications for which the installer metadata is the same as for the specified MSI installer are added to the user application category.

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 for the creating application category as you need.

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. It is 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 following Help topics:

- Kaspersky Endpoint Security for Windows Help
- Kaspersky Endpoint Security for Linux 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 a category and use it in the Application Control component configuration.

To create a category that includes executable files from selected devices:

1. In the main menu, go to **Operations** → **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. On 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** option.

4. Click **Add**.

5. In the window that opens, select a device or devices whose executable files will be used to create the 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 must select an algorithm for hash value computing by Kaspersky Next Expert View 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 10 Service Pack 2 for Windows and later versions support SHA256 computing. Computing of the MD5 hash function is supported by all versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Select either of the options of hash value computing by Kaspersky Next Expert View for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions, select the **SHA256** check box. We do not recommend that you add any categories created according to the criterion of the SHA256 hash of an executable file for versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows. This may result in failures in the security application operation. In this case, you can use the MD5 cryptographic hash function for files of the category.

- If any versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows are installed on your network, select the **MD5 hash**. You cannot add a category that was created based on the criterion of the MD5 checksum of an executable file for Kaspersky Endpoint Security 10 Service Pack 2 for Windows or later versions. In this case, you can use the SHA256 cryptographic hash function for files of the category.

If different devices on your network use both earlier and later versions of Kaspersky Endpoint Security 10, select both the **SHA256** check box and the **MD5 hash** check box.

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.

Viewing the list of application categories

You can view the list of configured application categories and the settings of each application category.

To view the list of application categories,

In the main menu, go to **Operations** → **Third-party applications** → **Application categories**.

The page with a list of application categories is displayed.

To view properties of an application category,

Click the name of the application category.

The properties window of the application category is displayed. The properties are grouped on several tabs.

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 following Help topics:

- Kaspersky Endpoint Security for Windows Help
- Kaspersky Endpoint Security for Linux Help

Adding event-related executable files to the application category

After you configure Application Control in the Kaspersky Endpoint Security for Windows 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 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**

    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.

    Select this option if you want to add only the details of the MD5 hash function of the executable file. Computing of the MD5 hash function is supported by Kaspersky Endpoint Security 10 Service Pack 1 for Windows and all earlier versions.

5. Click **OK**.

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 following Help topics:

- Kaspersky Endpoint Security for Windows Help
- Kaspersky Endpoint Security for Linux Help

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.

Creating installation packages of third-party applications from the Kaspersky database is only available under the 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 **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.
2. Click **Add**.
3. On the New package wizard page that opens, select the **Select an application from the Kaspersky database to create an installation package** option, and then click **Next**.
4. In the list of applications that opens, select the relevant application, and then click **Next**.
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 the End User License Agreement to continue installation, on the **End User License Agreement** page, follow the link on the vendor's website to read the End User License Agreement, and then select the **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement**.
7. On the **Name of the new installation package** page, in the **Package name** field, enter the name for the installation package, and then click **Next**.

Wait until the newly created installation package is uploaded to Administration Server. When the New package wizard displays the message informing you the package creation process was successful, click **Finish**.

The newly created installation package appears on the list of installation packages. You can select this package when creating or reconfiguring the *Install application remotely* task.

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 **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.
2. In the list of installation packages that opens, click the name of the relevant package.
3. On the properties page that opens, modify the 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:

By default, only a subset of the settings listed below is displayed. You can add the corresponding columns by clicking the **Filter** button and selecting columns 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.

- **Revoked**

  Displays the date and time when the update was revoked.

- **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.

- **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 revision number of the installation packages.

  - **Time**—Date and time the installation package settings were modified.

- **User**—Name of the user who modified the installation package settings.
- **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 then click the **Edit description** button. In the opened window, enter some text for the revision description.

Application tags

Kaspersky Next Expert View 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 **Operations** → **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 **Operations** → **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 **Operations** → **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 **Operations** → **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 **Operations** → **Third-party applications** → **Application tags**.
2. In the list, select the application tag that you want to delete.
3. 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.

Configuring Administration Server

This section describes the configuration process and properties of Administration Server.

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. For the Administration Server that is in the Kaspersky infrastructure, both primary and secondary Administration Servers on your network are secondary Servers. You can add a Windows-based Administration Server as well as a Linux-based Administration 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.

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 Next Expert View 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

You can make an Administration Server running on-premises function as a secondary Administration Server, thus establishing a "primary/secondary" hierarchy on your network. For the Administration Server that is in the Kaspersky infrastructure, both primary and secondary Administration Servers on your network are secondary Servers. You can add a Windows-based Administration Server as well as a Linux-based Administration Server.

To add a secondary Administration Server that is available for connection:

1. Make sure that the future secondary Administration Server has Kaspersky Security Center Web Console installed.

2. On the future secondary Administration Server, download the Administration Server certificate and save it so you can add it to the primary Administration Server during one of the steps of the Add secondary Administration Server wizard.

3. Perform the following actions via the Kaspersky Security Center Web Console on the future Secondary Administration Server (alternatively, you can prompt the administrator of the future Secondary Administration Server to perform these actions):

   a. Go to the properties of the future primary Administration Server by clicking the Administration Server name in the main menu.

      Alternately, you can go to the properties of the required Administration Server from the navigation pane. To do so, 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. In the navigation pane that opens, hover the mouse cursor over the name of the required Administration Server, and then click the settings icon (⚙).

   b. In the properties window 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 **Cloud Console** as the type of the primary Administration Server.

      The fields for settings to establish connection between secondary and primary Administration Servers become available.

   e. In the **HDS server address (from primary Administration Server on Cloud Console)** and **HDS server ports** fields, enter the address and port of the Kaspersky Next Expert View primary Administration Server.

      You can find HDS Server address and HDS Server port in the Kaspersky Next Expert View Administration Server, in the **Hierarchy of Administration Servers** section of the **General** tab of the properties window. You can copy and paste this data into the fields in the window of the secondary Administration Server.

   f. Click the **Specify primary Administration Server certificate** button, and then select the certificate.

      You can download this certificate from Kaspersky Next Expert View Administration Server, in the **Hierarchy of Administration Servers** section of the **General** tab of the properties window, by clicking the **View Administration Server certificate** button.

   g. Click the **Specify Hosted Discovery Service certificates** button, and then select the certificate.

      You can download this certificate from Kaspersky Next Expert View Administration Server, in **Hierarchy of Administration Servers** section of the **General** tab of the properties window, by clicking the **HDS root CA certificate** button.

   h. If you use a proxy server to connect to the Kaspersky Next Expert View Administration Server (that is, the primary Server in the hierarchy that you have built), specify this and enter the proxy server credentials.

   i. Select the **Connect primary Administration Server to secondary Administration Server in DMZ** option if the secondary Administration Server is in a demilitarized zone.

   j. Click **Save** to save the changes and exit the window.

4. In the Kaspersky Next Expert View main menu, click the Administration Server name.

5. On the properties page that opens, click the **Administration Servers** tab.

6. Select the check box next to the name of the administration group to which you want to add the secondary Administration Server.

7. 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.

8. Fill in the following fields:

   - **Secondary Administration 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 Administration Server address (optional)**

     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.

9. If you use a proxy server to connect to the Kaspersky Next Expert View Administration Server (that is, the future primary Server), specify this and enter the proxy server credentials.

10. Follow the steps of the wizard.

After the wizard finishes, the "primary/secondary" hierarchy is built. The primary Administration Server starts receiving connection from the secondary Administration Server 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.

Configuring storage term of events concerning to the deleted devices

In Kaspersky Next Expert View, events are stored in an event repository. You cannot configure how many events to store in the event repository.

In the **Events repository** section of the Administration Server properties window, you can configure the maximum storage term of events concerning to the deleted devices. The maximum storage term is 1000 days.

To configure the number of days to store events relating to the deleted devices:

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.

3. Enable **Store events after devices are deleted** option.

4. In the **Maximum storage period (days)** edit box specify the number of days to store events relating to the deleted devices.

The number of days to store events concerning to the deleted devices is limited by the specified value.

Additionally, you can change the settings of any task to save events related to the task progress, or save only task execution results. 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.

Aggregate emails about events

During the operation, Kaspersky Next Expert View and managed Kaspersky applications generate events. 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, Kaspersky Next Expert View can assign different levels of severity to events of the same type.

Kaspersky Next Expert View automatically sends, by email, notifications about events. Kaspersky Next Expert View sends notifications about events listed in the **Administration Server properties** window, on the **Event configuration** tab. Common notification settings are used for all event types.

To limit the number of emails that have to be sent, Kaspersky Next Expert View, during specific periods, aggregates events with the same severity level. Values of the periods are managed by Kaspersky specialists. If necessary, you can view the information about the aggregation intervals by **clicking this link**.

After sending a notification about a new event with a specific severity level, Administration Server performs the following actions:

1. Activates a 15-minutes counter.

2. In 15 minutes:

   - If no events of the same or a lower severity level occur, the counter is reset.

   - If at least one event with the same or a lower severity level occurs, sends recipients one aggregated email with information about the events, and then activates another counter with a three-hour interval.

     In this case, Administration Server performs one of the following actions:

     - If during these three hours no events of the relevant (or lower) severity level occur, both counters are reset.

     - If at least one event with the same or lower severity level occurs, sends recipients one aggregated email with the information about the events, and reactivates the three-hour counter.

If at least one event with a higher severity level occurs during one of the intervals (15 minutes or 3 hours), Administration Server sequentially performs the following actions:

a. Sends recipients one aggregated email with the information about previously accumulated events without waiting until the end of the interval.

b. Sends recipients an email about the new event with the higher severity level.

c. Resets the activated counters.

d. Activates a new 15-minutes counter, and the scenario described here is restarted.

As a result, recipients get aggregated email messages according to the following template: "<Number> <Severity_level> (and lower-level) events have occurred".

If you want to receive notifications from users immediately, you can configure integration between Kaspersky Next Expert View and SIEM, and then configure notifications of the necessary events from SIEM.

Limitations on management of secondary Administration Servers running on-premises through Kaspersky Next Expert View

After you switch to a secondary Administration Server running on-premises by using the corresponding option in Kaspersky Next Expert View, the application imposes specific limitations on management of this secondary Administration Server. The following settings related to the Kaspersky Next Expert View operation become unavailable for the user:

- In the settings of Network Agent policies and Administration Server policies, the **Event configuration** and **Application settings** tabs are unavailable; no new policies can be created.
- In the settings of Network Agent tasks and Administration Server tasks, the **Event configuration** and **Application settings** tabs are unavailable; no new tasks can be created.
- Management of Network Agent and Administration Server is unavailable, as well as the properties window of the secondary Administration Server.
- The quick start wizard is unavailable.
- The storage and notification settings for Network Agent and Administration Server events cannot be modified.
- The **Current application versions** section is unavailable.
- The **Installation packages** section is unavailable.

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: **Assets (Devices)**, **Policies**, **Tasks**, and **Distribution points**. Otherwise, the groups are grayed-out.

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 name of the primary Administration Server.
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.

Configuring the interface

You can configure the Kaspersky Next Expert View interface to display and hide sections and interface elements, depending on the features that you use.

To configure the Kaspersky Next Expert View interface in accordance with the currently used set of features:

1. In the main menu, go to **Settings** → **Interface options**.
2. In the **Interface options** window that opens, enable or disable the options:
   - **Show data encryption and protection**

     You can use this option to hide or show the **Operations** → **Data encryption and protection** section in the interface. Kaspersky Next Expert View saves the value of this option only for your own user account while the other user can set a different value.
   - **Show MDR features**

     You can use this option to hide or show the **Monitoring** → **Incidents** section in the interface. Kaspersky Next Expert View saves the value of this option only for your own user account while the other user can set a different value.
3. Set the number of devices that Kaspersky Next Expert View displays in policy distribution results.
4. Click the **Save** button.

The console interface settings are configured according to your preferences.

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.

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.
4. On the menu line, click **New virtual Administration Server**.

5. On the page that opens, define the **Name of virtual Administration Server**.

6. Click the **Save** button.

The new virtual Administration Server is created, added to the administration group and displayed on the **Administration Servers** tab.

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 is not included in the **Access rights** list in the properties of 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

When you assign an administrator, make sure that you grant access to a single virtual Administration Server. An administrator with access to multiple virtual Administration Servers cannot sign in to Kaspersky Next Expert View.

An administrator of a virtual Administration Server signs in to Kaspersky Next Expert View the same way as signing in to the primary Administration Server. Kaspersky Next Expert View 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.
- The created account of the virtual Server administrator is not included in the **Access rights** lists in the properties of any Servers—primary or secondary.
- 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**.

   Selecting two or more virtual Servers automatically grants access to their primary Administration Server. In that case, this selection cannot be cleared without clearing the virtual Servers' selection.
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.

   > When assigning roles to a user, in the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab. If you select the **Groups** tab, and then assign roles to the group where the user is a member, the user will not be able to log in to Kaspersky Next Expert View.

The application assigns the new role 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.

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 Next Expert View, 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. In the main menu, click the Administration Server.
2. On the page that opens, proceed to the **Administration Servers** tab.
3. Select the virtual Administration Server that you want to delete.
4. On the menu line, click the **Delete** button.

The virtual Administration Server is deleted.

Monitoring and reporting

This section describes the monitoring and reporting capabilities of Kaspersky Next Expert View. These capabilities give you an overview of your infrastructure, protection statuses, and statistics.

After Kaspersky Next Expert View 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 Next Expert View.

Prerequisites

After you deploy Kaspersky Next Expert View in the corporate network, you can start to monitor the security status of the network using Kaspersky Security Center and generate reports.

Stages

Configuring monitoring and reporting on 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) of events on client devices

   > We recommend configuring automatic event forwarding to a SIEM system for long-term storage of Kaspersky application events. This also enables prompt email notifications about security events and faster response to them.

3. **Changing the response of your security network to the Virus outbreak event**

   You can change the specific thresholds in the Administration Server properties. You can also create a stricter policy that will be activated or create a task that will be run at the occurrence of this event.

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. **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 Next Expert View provides the following types of monitoring and reporting on your organization's network:

- Dashboard
- Reports
- Event selections

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 Next Expert View interface, for configuration.

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 Next Expert View, in the **Monitoring** → **Dashboard** section.

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 Next Expert View 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**.
2. Click the **Add or restore widget** button.
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.
4. Click **Add**.

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.

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 Next Expert View (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 Next Expert View, 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 Next Expert View 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 Next Expert View, in the **Monitoring** → **Reports** section.

By default, reports include information for the last 30 days.

Kaspersky Next Expert View 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.
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.
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.
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.

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.
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.

       Note that the Kaspersky Next Expert View interface can display a maximum of 2500 entries. If you need to view a greater number of events, use the report export feature.
     - **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 Next Expert View 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.
3. Click the **Export report** button.
4. In the opened window, 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.

   - **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.
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 only in English, other localizations are not available.

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.

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**.

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 Monday 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.

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 disabled.

     - **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.

     - **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.

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.

    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.

Events and event selections

This section provides information about events and event selections, about the types of events that occur in Kaspersky Next Expert View components, and about managing frequent events blocking.

About events in Kaspersky Next Expert View

Kaspersky Next Expert View 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 export this information to external SIEM systems. Exporting event information to external SIEM systems enables administrators of SIEM systems to promptly respond to security system events that occur on managed devices or groups of devices.

Events by type

In Kaspersky Next Expert View, there are the following types of notifications:

- 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:

- Components of the Kaspersky Next Expert View:
  - 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 Next Expert View. 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 Next Expert View components

Each Kaspersky Next Expert View component has its own set of event types. This section lists types of events that occur in Kaspersky Next Expert View 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 Next Expert View 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 Next Expert View database.
- **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.

Administration Server events

This section contains information about the events related to the Administration Server.

Administration Server critical events

The table below shows the events of Kaspersky Next Expert View Administration Server that have the **Critical** 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.

Event type display name	Event type ID	Event type	Description	Default storage term
License limit has been exceeded	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Once a day Kaspersky Next Expert View checks whether a license limit is exceeded. 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. Even when this event occurs, client devices are protected. You can respond to the event in the following ways: • Look through the managed devices list. Delete devices that are not in use. • Provide a license for more devices (add a valid activation code or a key file to Administration Server). Kaspersky Next Expert View determines the rules to generate events when a license limit is exceeded.	180 days
Virus outbreak	26 (for File Threat Protection)	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. You can respond to the event in the following ways: • Configure the threshold in the Administration Server properties. • Create a stricter policy that will be activated, or create a task that will be run, at the occurrence of this event.	180 days
Virus outbreak	27 (for Mail Threat Protection)	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. You can respond to the event in the following ways: • Configure the threshold in the Administration Server properties. • Create a stricter policy that will be activated, or create a task that will be run, at the occurrence of this event.	180 days
Virus outbreak	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. You can respond to the event in the following ways: • Configure the threshold in the Administration Server properties. • Create a stricter policy that will be activated, or create a task that will be run, at the occurrence of this event.	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. 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

Event type display name	Event type ID	Event type	Description	Default storage term
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
Limited functionality mode	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Events of this type occur when Kaspersky Next Expert View starts to operate with basic functionality, without Vulnerability and patch management and without Mobile Device Management features. Following are causes of, and appropriate responses to, the event: • License term has expired. Provide a license to use the full functionality mode of Kaspersky Next Expert View (add a valid activation code or a key file to Administration Server). • 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
License expires soon	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Events of this type occur when the commercial license expiration date is approaching. Once a day Kaspersky Security Center checks whether the license has expired on the devices. 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. When the commercial license expires, Kaspersky Next Expert View provides only basic functionality. You can respond to the event in the following ways: • Make sure that a reserve license key is added to Administration Server. • 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
MDM certificate has expired	4132	KLSRV_CERTIFICATE_EXPIRED	Events of this type occur when the client certificate on mobile devices expires.	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 Next Expert View patches and does not concern modules of Kaspersky managed applications. The event provides the reason that the seamless updates are not installed.	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

Administration Server functional failure events

The table below shows the events of Kaspersky Next Expert View 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
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 Next Expert View 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. You can respond to the event in the following ways: • Look through the managed devices list. Delete the third-party application from devices on which the application is not in use. • Use a third-party license for more devices. 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
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

Administration Server warning events

The table below shows the events of Kaspersky Next Expert View Administration Server that have the **Warning** 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.

Event type display name	Event type ID	Event type	Description	Default storage term
License limit has been exceeded	4098	KLSRV_EV_LICENSE_CHECK_100_110	Once a day Kaspersky Next Expert View checks whether a license limit is exceeded. 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. Even when this event occurs, client devices are protected. You can respond to the event in the following ways: • Look through the managed devices list. Delete devices that are not in use. • Provide a license for more devices (add a valid activation code or a key file to Administration Server). Kaspersky Next Expert View determines the rules to generate events when a license limit is exceeded.	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. Most often, this happens when a managed device is decommissioned. You can respond to the event in the following ways: • Manually remove the device from the list of managed devices. Specify the time interval after which the **Device has remained inactive on the network for a long time** event is created by using Kaspersky Next Expert View. • Specify the time interval after which the device is automatically removed from the group by using Kaspersky Next Expert View.	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. Although cloning is not supported in Kaspersky Next Expert View, this event may occur if you perform cloning using a third-party tool. To avoid the event, when copying the image of a device with Network Agent installed, you have to meet the following recommendations: • On the reference device, stop the Network Agent service and run the klmover utility with the -dupfix key. Avoid any subsequent runs of Network Agent service until the image capturing operation completes. • Make sure that the klmover utility will be run with the -dupfix key before (mandatory requirement) the first run of the Network Agent service on target devices, at the first launch of the operating system after the image deployment. The utility klmover is included in the installation package of Network Agent. If you capture the image of a device without Network Agent installed, perform image deployment on target devices and then deploy Network Agent. You have to provide access to the network folder with stand-alone installation packages from a device.	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
Limit of installations will soon be reached 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. You can respond to the event in the following ways: • If the third-party application is not in use on some of the managed devices, delete the application from these devices. • 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. You can manage license keys of third-party applications using the functionality of licensed applications groups.	90 days
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. Following might be the causes and appropriate responses to the event: • Automatic reissue was initiated for a certificate for which the **Certificate has been requested** 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. • 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
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. After removing a certificate, mobile devices connected via this certificate will fail to connect to Administration Server. This event might be helpful when investigating malfunctions associated with the management of mobile devices.	90 days
APNs certificate has expired	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Events of this type occur when an APNs certificate expires. You need to manually renew the APNs certificate and install it on an iOS MDM Server.	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. When the APNs certificate expires, you need to manually renew the APNs certificate and install it on an iOS MDM Server. We recommend that you schedule the APNs certificate renewal in advance of the expiration date.	90 days

Event type display name	Event type ID	Event type	Description	Default storage term
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. 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
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). Following might be the causes and appropriate responses to the event: • 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"). • 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
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. Read the details in the event description and respond accordingly. If you cannot find the solution to an issue on your own, we recommend that you contact Kaspersky Technical Support.	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
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. Read the operating system log on the device where the secondary Administration Server is installed and respond accordingly.	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. Read the operating system log on the device where the primary Administration Server is installed and respond accordingly.	90 days
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

Event type display name	Event type ID	Event type	Description	Default storage term
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. Approve or decline the updates by using Kaspersky Security Center Web Console.	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. You can respond to the event in the following ways: • Change the maximum number of events stored in the Administration Server database • 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. You can respond to the event in the following ways: • Change the allowed maximum number of events to be stored in the Administration Server database • 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 Kaspersky Next Expert View 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
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. Even when a licensing limit is exceeded, client devices are protected. You can respond to the event in the following ways: • Look through the managed devices list. Delete devices that are not in use. • Provide a license for more devices (add a valid activation code or a key file to Administration Server). Kaspersky Next Expert View determines the rules to generate events when a license limit is exceeded.	30 days

Event type display name	Event type ID	Event type	Description	Default storage term
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
Device has been automatically moved according to a rule	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	Events of this type occur when devices have been assigned to a group according to device moving rules.	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
Limit of installations will soon be exceeded (more than 90% is used up) for one of the licensed applications groups	4128	KLSRV_INVLICPROD_EXPIRED_SOON	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. You can respond to the event in the following ways: • If the third-party application is not in use on some of the managed devices, delete the application from these devices. • 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. You can manage license keys of third-party applications using the functionality of licensed applications groups.	30 days
Files have been found to send to Kaspersky for analysis	4131	KLSRV_APS_FILE_APPEARED		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. For information on the FCM token rotation, please refer to the Firebase service documentation.	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
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
Connection to the primary Administration Server has been established	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 days
Databases have been updated (In Kaspersky Next Expert View, this event type is available only for a secondary Administration Server.)	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 added to the group	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	Events of this type occur when devices have been assigned to a group according to device moving rules.	30 days
KSN Proxy has started; KSN availability check has completed successfully	7718	KSNPROXY_STARTED_CON_CHK_OK		30 days

Event type display name	Event type ID	Event type	Description	Default storage term
KSN Proxy has stopped	7720	KSNPROXY_STOPPED		30 days
Audit: Connection to the Administration Server has been established	4147	KLAUD_EV_SERVERCONNECT		30 days
Audit: Connection to Administration Server has been terminated	4151	KLAUD_EV_SERVERDISCONNECT		30 days
Audit: Object has been modified	4148	KLAUD_EV_OBJECTMODIFY	This event tracks changes in the following objects: • Administration group • Security group • User • Package • Task • Policy • Server • Virtual Server	30 days
Audit: Object properties have been modified	4152	KLAUD_EV_OBJECTPROPMODIFIED	This event tracks changes in the following properties: • User • License • Server • 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: 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: Encryption keys have been imported or exported from Administration Server	5100	KLAUD_EV_DPEKEYSEXPORT		30 days
Audit: Test connection to SIEM server succeeded	5110	KLAUD_EV_SIEM_TEST_SUCCESS		30 days
Audit: User permissions have been modified	4153	KLAUD_EV_OBJECTACLMODIFIED	This event occurs when user permissions have been modified	30 days

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 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
Update installation error	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Events of this type occur if automatic updating and patching for Kaspersky Next Expert View components was not successful. The event does not concern updates of the managed Kaspersky applications. 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
Failed to install the third-party software update	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Events of this type occur if Vulnerability and patch management and Mobile Device Management features are in use, and if update of third-party software was not successful. Check whether the link to the third-party software is valid. Read the event description.	30 days
Failed to install the Windows Update updates	7717	KLNAG_EV_WUA_INSTALL_ERROR	Events of this type occur if Windows Updates were not successful. Configure Windows Updates in a Network Agent policy. 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 install root certificates	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	The event contains the description of the certificates installation error.	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
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 Kaspersky Security Center 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	Default storage term
Warning has been returned during installation of the software module update	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 days
Third-party software update installation has completed with a warning	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 days
Third-party software update installation has been postponed	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 days
Security issue has occurred	549	GNRL_EV_APP_INCIDENT_OCCURED	30 days
Sudoers file found does not match reference value	7724	KLNAG_EV_SUDOER_DIFFERENT	30 days
KSN Proxy has started. Failed to check KSN for availability	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 days
User management: warnings	7722	KLNAG_EV_USR_MNG_WRN	30 days

Network Agent informational events

The table below shows the events of Kaspersky Security Center 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
Update for software modules has been installed successfully	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 days
Installation of update for software modules has started	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 days
Application has been installed	7703	KLNAG_EV_INV_APP_INSTALLED	30 days
Application has been uninstalled	7704	KLNAG_EV_INV_APP_UNINSTALLED	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
Third-party application has been installed	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	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
New device has been added	7708	KLNAG_EV_DEVICE_ARRIVAL	30 days
Device has been removed	7709	KLNAG_EV_DEVICE_REMOVE	30 days
Device has been detected	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 days
Device has been authorized	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	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
Certificate received for Web Server HTTPS port	—	WEB_SERVER_CERTIFICATE_RENEWED	30 days
Windows Desktop Sharing: File has been read	7712	KLUSRLOG_EV_FILE_READ	30 days
Windows Desktop Sharing: File has been modified	7713	KLUSRLOG_EV_FILE_MODIFIED	30 days

Event type display name	Event type ID	Event type	Default storage term
Windows Desktop Sharing: Application has been started	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 days
Windows Desktop Sharing: Started	7715	KLUSRLOG_EV_WDS_BEGIN	30 days
Windows Desktop Sharing: Stopped	7716	KLUSRLOG_EV_WDS_END	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
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

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 Next Expert View interface, for configuration.

Event selections are available in Kaspersky Next Expert View in the **Monitoring** → **Event selections** section.

By default, event selections include information for the last seven days.

Kaspersky Next Expert View has a default set of event (predefined) selections:

- Events with different importance levels:
  - **Critical events**
  - **Functional failure**
  - **Warnings**
  - **Informational messages**
- **User requests** (events of managed applications)
- **Recent events** (over the last week)

- **Audit events**

  In Kaspersky Next Expert View, audit events related to service operations in your workspace are displayed. These events are conditioned by actions of Kaspersky specialists. These events, for example include the following: Administration Server ports changing; Administration Server database backup; creation, modification, and deletion of user accounts.

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 Next Expert View 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**.
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.
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 the **Monitoring** → **Event selections**.
2. Select the check box next to the event selection that you want to edit.
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.
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.

     c. 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.

Exporting an event selection

Kaspersky Next Expert View 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 Next Expert View (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 Next Expert View 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.
3. In the displayed window, you can do the following:
   - View the information about the selected event
   - Go to the next event and the previous event in the event selection result
   - 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 Next Expert View allows you to save events from an event selection to a TXT file.

To export events to a file:

1. Start an event selection.
2. Select the check box next to the required event.
   You can also select several events or the entire event selection.
3. Click the **Export to file** button.

The selected event is exported to a TXT file.

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.

Logging information about events for tasks and policies

This section offers recommendations on how to minimize the number of events for tasks and policies stored in the database of Kaspersky Next Expert View. If the storage limit is exceeded, new events overwrite old ones. As a result, critical events may disappear. Also, the Administration Server warning event named **The limit on the number of events in the database is exceeded, the events have been deleted** may occur. In these cases, we recommend that you follow the instructions in this section.

As a result, you will increase the speed of executing scenarios associated with the analysis of the events. Also, these recommendations help you lower the risk that critical events will be overwritten by a large number of events.

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 frequently (for example, more than once per week), 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, Kaspersky Next Expert View stores only information about task launch, progress, and completion (successful, with a warning, or with an error) from each device on which the task is run.
- **Save only task execution results**. In this case, Kaspersky Next Expert View stores only information about task completion (successful, with a warning, or with an 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, we recommend selecting only the most critical events in the policy settings and enabling their logging. You are advised to disable the logging of all other 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 if events about changes in the intermediate statuses of group tasks and events about applying policies occupy a large share of all events in the Kaspersky Next Expert View database.

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.

To delete events from a device events list:

1. Open the device list.
   - For managed devices: **Asset management** → **Assets (Devices)**.
   - For unassigned devices: **Discovery & deployment** → **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. Then click the **Delete** button.

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.

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 Windows, 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 settings icon ( ) next to the name of the required Administration Server.

   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 the **Save** button.

   - 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 the **Save** button.

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 settings icon ( ) next to the name of the required Administration Server.

   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.

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:

- On-screen notifications
- Email notifications.

Onscreen notifications

On-screen notifications are available in the drop-down panel that opens when you click the notifications icon ( ) and in Notification center. They are assigned one of the following importance categories: **Critical**, **Warning**, or **Info**.

> 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 Next Expert View 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.

Email notifications.

Kaspersky Next Expert View 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.

Upon receiving notifications by email, you can decide on your response to an event. This response should be the most appropriate for your organization's network.

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 Next Expert View 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 Next Expert View and they set different interface languages, Kaspersky Next Expert View 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 Next Expert View.

  To provide information relevant to your network protection configuration, Kaspersky Next Expert View 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 Next Expert View.

- 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 Next Expert View 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 announcements

Announcements include two types of information:

- Security-related announcements
- Marketing announcements

You can disable the announcements of each type separately.

You cannot disable the security-related announcements in the trial mode of Kaspersky Next Expert View.

Disabling security-related 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 Disabled** position.
4. Click the **Save** button.
   Security-related announcements are disabled.

Disabling marketing announcements

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.

To disable marketing announcements:

1. In the main menu, click the Administration Server name.
   The Administration Server properties window opens.
2. On the **General** tab, select the **KSN settings** section.
3. Switch the toggle button to the **Use Kaspersky Security Network Disabled** option.
4. Click the **Save** button.
   Marketing announcements are disabled.

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. 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 **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**.

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**.

When specified conditions are met, the managed device is assigned the *Warning* status.

Configuring notification delivery

You can configure email notification about events occurring in Kaspersky Next Expert View.

To configure notification delivery of events occurring in Kaspersky Next Expert View:

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 define the email notification settings:

   Recipients (email addresses)

   The email addresses to which the Kaspersky Next Expert View will send notifications. You can specify multiple addresses in this field, by separating them with semicolons.

   > You can specify no more than 24 email addresses.

3. Click the **Send test message** button to check whether you configured notifications properly: the application sends a test notification to the email addresses that you specified.

4. Click the **OK** button to close the Administration Server properties window.

The saved notification delivery settings are applied to all events that occur in Kaspersky Next Expert View.

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.

Receiving license expiration warning

To add a Kaspersky Endpoint Security for Business Select license key 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 **License keys** section.

3. Click **Select**.

4. In the window that opens, select your license and click **OK**.

   Alternatively, if no license is displayed, you can click **Add new license key** and use your activation code.

The license is added to the Administration Server repository. This makes the Administration Server generate a critical event *License expires soon* one day before the license term expires and a critical event *Limited functionality mode* after the license term expires. If you want, you can configure notification delivery.

> If you add a Kaspersky Endpoint Security for Business Select license key to the Administration Server repository, then the license is considered used on one device.

Cloud Discovery

Kaspersky Next Expert View 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 Next Expert View under a Kaspersky Next EDR Optimum or Kaspersky Next XDR Optimum 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, which provides 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 Next Expert View gets information about the use of cloud services from all of the managed devices that are protected only by the security policies or 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. Open Kaspersky Next Expert View Management Console.
2. In the main menu, go to **Monitoring** → **Dashboard**.
3. On the **Cloud Discovery** widget, click the **Enable** button.
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. Open Kaspersky Next Expert View Management Console.
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, which displays information about attempts to gain access to cloud services. The widget also displays the risk level of each cloud service. Kaspersky Next Expert View 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. Open Kaspersky Next Expert View Management Console.
2. In the main menu, go to **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 Next Expert View under a Kaspersky Next EDR Optimum or Kaspersky Next XDR Optimum 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. Among other considerations, 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.

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 **Operations** → **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 Next Expert View 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 Next Expert View 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 **Operations** → **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 **Operations** → **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.

Working with Kaspersky Next Expert View 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 Next Expert View 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 Next Expert View 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.

After you activated Administration Server under your Kaspersky Next XDR Optimum license and deployed the license key to your managed applications, 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.

Also, you can use the functionality of Kaspersky Next XDR Optimum in trial mode. To do this, you must create a trial workspace, and then deploy the trial license key to your managed applications. The Kaspersky Next XDR Optimum functionality will be available during the validity period of your trial workspace.

Integrations for responding to alerts

You can configure integrations with the following solutions for responding to threats:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

To configure the integrations, the following conditions must be met:

- When using the functionality of Kaspersky Next XDR Optimum in commercial mode, you must:
  - Have a commercial workspace, and the **Read** and **Write** rights for the **General features: Application integration** functional area.
  - Activate Administration Server under a Kaspersky Next XDR Optimum license.
  - Deploy the Kaspersky Next XDR Optimum license key to your managed applications to perform response actions.

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 key to secondary and virtual Administration Servers is not supported.

- When using the functionality of Kaspersky Next XDR Optimum in trial mode, you must create a trial workspace, and then deploy the trial license key to your managed applications. The Kaspersky Next XDR Optimum functionality will be available during the validity period of your trial workspace.

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.

The integration with Active Directory for responding to alerts, the ADFS integration, 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 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. Select the **Distribution points** section, and then click the name of the required distribution point.

3. In the properties window that opens, select the **Connection gateway** section, and then enable the **Connection gateway** option.

4. Select the **Active Directory** section.

5. 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.

6. Create a connection to the Active Directory domain controller by clicking the **Add connection** button.

7. In the window that opens, specify the following parameters for the connection:

   - **Domain controller address**

     Computer name, for example: `server.example.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: `example.com`

  Also, you can specify SAM or NetBIOS name, for example: `example`

  Use lowercase letters. If you create several connections for the Administration Server or a distribution point, specify different names for each connection.

  > We do not recommend using the address of a specific domain controller and a short domain name (SAM or NetBIOS).
  > 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.

8. 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 the way you connect to Active Directory: **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. 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.

9. Then click the **Create** button.

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 Next Expert View, 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. In the **Integrations** section, select **KASAP**.

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.

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. 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

In commercial mode, to enable the functionality of alert aggregation, you have to activate Administration Server under a Kaspersky Next XDR Optimum license, and then deploy the Kaspersky Next XDR Optimum license key to your managed applications. 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.

In trial mode, you must have a trial workspace, and deploy the trial license key to your managed applications. The functionality of alert aggregation will be available during the validity period of your trial workspace.

Aggregation groups alerts that may belong to the same incident, which makes the investigation process easier. 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 the **Monitoring** → **Alerts** section.
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.

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** → **Assets (Devices)**.
   - If the device belongs to the Unassigned devices group, in the main menu, go to **Discovery & deployment** → **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 application list, 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 Kaspersky Security 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

You can download trace files from a client device only if one of the following conditions is met: the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, a push server is in use, or a connection gateway is in use. Otherwise, the downloading is not possible.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

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.

   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

You can download application settings from a client device only if one of the following conditions is met: the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, a push server is in use, or a connection gateway is in use. Otherwise, the downloading is not possible.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

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

You can download system information from a client device only if one of the following conditions is satisfied: the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, a push server is in use, or a connection gateway is in use. Otherwise, the downloading is not possible.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

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.

> 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

You can download event logs from a client device only if one of the following conditions is satisfied: the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, a push server is in use, or a connection gateway is in use. Otherwise, the downloading is not possible.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

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.
     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 an application and downloading the results

To start diagnostics for an application 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 the application for which you want to run remote diagnostics.

   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 that you want to run on the client device. 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.

Generating a dump file for an application

An application dump file allows you to view the parameters of the application running on a client device at a point in time. This file also contains information about modules that were loaded for an application.

Generating dump files is available only for 32-bit processes running on Windows-based client devices. For client devices running Linux and for 64-bit processes this feature is not supported.

To create a dump file for an application:

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 **Generating the process dump file** section, specify the executable file of the application for which you want to generate a dump file.

4. Click the **Download** button to save the dump file for the specified application.

   If the specified application is not running on the client device, the error message will be displayed.

Running remote diagnostics on a Linux-based client device

Kaspersky Next Expert View 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 Next Expert View, 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.

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

This section provides a scenario for configuring the export of events from Administration Server to external SIEM systems. Exporting event information to external SIEM systems enables administrators of SIEM systems to promptly respond to security system events that occur on managed devices or groups of devices.

Prerequisites

Before you start configuring the export of events in the Kaspersky Next Expert View:

- Learn more about the methods of event export.
- Make sure that you know the values of the system settings.

> You can perform the steps of this scenario in any order.

Stages

The process of the export of events to a SIEM system consists of the following stages:

- **Configuring the SIEM system to receive events from Kaspersky Next Expert View**

  You have to configure receiving events from Kaspersky Next Expert View in the SIEM system.

- **Marking events for export**

  You have to mark which events you want to export to the SIEM system. First of all, mark the general events that occur in all managed Kaspersky applications. Additionally, you can mark the events for specific managed Kaspersky applications.

- **Configuring Kaspersky Next Expert View for export of events to a SIEM system**

  You have to configure Kaspersky Next Expert View to start export of events to a SIEM system.

Results

After configuring export of events to a SIEM system you can view export results if you selected events which you want to export.

Before you begin

When setting up the automatic export of events in the Kaspersky Next Expert View, 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 Next Expert View.

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 Next Expert View and your SIEM system server. You specify this value in the Kaspersky Next Expert View settings and in the receiver settings of your SIEM system.

- **Protocol**

  Protocol used for transferring messages from Kaspersky Next Expert View to your SIEM system. You specify this value in the Kaspersky Next Expert View settings and in the receiver settings of your SIEM system.

About event export

Kaspersky Next Expert View 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 Next Expert View to external SIEM systems involves two parties: an event sender, Kaspersky Next Expert View, and an event receiver, a SIEM system. To successfully export events, you must configure this in your SIEM system, Administration Console and in the Kaspersky Next Expert View. It does not matter which side you configure first. You can either configure the transmission of events in the Kaspersky Next Expert View, and then configure the receipt of events by the SIEM system, or vice versa.

Syslog format of event export

You can send events in the Syslog format to any SIEM system. Using the Syslog format, you can relay any events that occur on the Administration Server and in Kaspersky applications that are installed on managed devices. When exporting events in the Syslog format, you can select exactly which types of events will be relayed to the SIEM system. Receipt of events by the SIEM system

Receipt of events by the SIEM system

The SIEM system must receive and correctly parse the events received from Kaspersky Next Expert View. 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.

Configuring an event export in a SIEM system

The process of exporting events from Kaspersky Next Expert View to external SIEM systems involves two parties: an event sender, Kaspersky Next Expert View, and an event receiver, a SIEM system. You must configure the export of events in your SIEM system and in the Kaspersky Next Expert View.

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 Next Expert View, you must set up the receiver in your SIEM system. In general, the following settings must be specified in the SIEM system:

- **Port**

  Specify the port number to connect to Kaspersky Next Expert View. This port must be the same as the port you specify in Kaspersky Next Expert View during configuration with a SIEM system.

- **Message protocol or source type**

  Specify the Syslog format.

Depending on the SIEM system that you use, you may have to specify some additional receiver settings.

Message parser

Exported events are passed to SIEM systems as messages. These messages must be properly parsed so that information on the events can be used by the SIEM system. Message parsers are a part of the SIEM system—they are used to split the contents of the message into the relevant fields, such as event ID, severity, description, parameters, and so on. This enables the SIEM system to process events received from Kaspersky Next Expert View so that they can be stored in the SIEM system database.

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.

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** → **Assets (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. Do one of the following:
   - In the main menu, click the Administration Server name.
   - In the main menu, 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 Next Expert View to external systems.

In Kaspersky Next Expert View, 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 Next Expert View is configured so that it sends events to the SIEM system. Kaspersky Next Expert View 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 Next Expert View 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 Next Expert View.

To configure export to SIEM systems in the Kaspersky Next Expert View:

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 **SIEM** section, and then click the **Settings** link.

3. In the right pane that opens, **specify the export settings**.

   - In the **SIEM system server address** field, specify the IP address of the server on which the currently used SIEM system is installed.

     Check this value in your SIEM system settings.

   - In the **SIEM system port** field, specify the port number used to establish a connection between Kaspersky Next Expert View and your SIEM system server.

     You specify this value in the Kaspersky Next Expert View settings and in the receiver settings of your SIEM system.

   - In the **Protocol** list, the value is preselected. You can use only TLS over TCP protocol for transferring messages to the SIEM system.

   - In the **Server authentication** drop-down list, select one of the following items:

     - **Trusted certificates**, and then click the **Browse for CA certificates file** button that displays to upload the trusted certificate.

       You can receive a complete certificate chain (including the root certificate) from a trusted certification authority (CA) and upload the file to Kaspersky Next Expert View. Kaspersky Next Expert View checks whether the certificate chain of the SIEM system server is also signed by a trusted CA or not.

     - **SHA fingerprints**, and then in the **Thumbprints** field, enter the SHA1 thumbprint, and click the **Add** button.

       You can specify SHA1 thumbprints of the complete certificate chain of the SIEM system (including the root certificate) in Kaspersky Next Expert View.

   - Click the **Add Subject name/Subject alternative name** link.

     The link is only displayed if you selected the **Trusted certificates** item in the **Server authentication** drop-down list.

Subject name is a domain name for which the certificate is received. Kaspersky Next Expert View 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 **Subject name/Subject alternative name** field. If any of the specified subject names matches the subject name of the SIEM system certificate, Kaspersky Next Expert View validates the SIEM system server certificate.

- Click the **Add client authentication** link, and then, in the **If you do not have any certificate, you can generate one** drop-down list, select one of the following:

  - **Generate key**, and then click the **Generate** button if you want to generate a self-signed certificate in Kaspersky Next Expert View. As a result, Kaspersky Next Expert View stores the generated self-signed certificate, and you can pass the public part of the certificate or SHA1-fingerprint to the SIEM system.

    By using the setting, you generate a certificate to authenticate Kaspersky Next Expert View. Thus, you will use a self-signed certificate issued by Kaspersky Next Expert View. In this case, you can use both a trusted certificate and a SHA fingerprint to authenticate the SIEM system server.

  - **Insert certificate** if you want to use a certificate that you received from any source, for example, from any trusted CA.

    Then specify the certificate and its private key by doing the following:

    a. In the **Client certification** drop-down list, select the certificate type:

    - **X.509 certificate PEM**
    - **X.509 certificate PKCS12**

    b. In the **File with certificate** field, upload a file with a certificate.

    c. If you selected **X.509 certificate PEM**, in the **File with key** section that displays, upload a file with a private key.

    The file with a certificate and the file with a private key do not depend on each other and the order of loading the files is not significant.

    d. If the private key is encoded, specify the password for decoding in the **Password or certificate verification** field. Otherwise, you can leave the filed empty.

- In the **Data format** section, the **System log** value is preselected.

  You can only specify the limit on the length of a message sent to SIEM in the **Maximum message size, in bytes** field. If the limit is exceeded, the message is cut off.

4. 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**.

5. Switch the option to the **Automatically export events to SIEM system database** position.

6. To check that the SIEM system connection is configured, click the **Check connection** button.

   The connection status will be displayed.

7. 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 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.

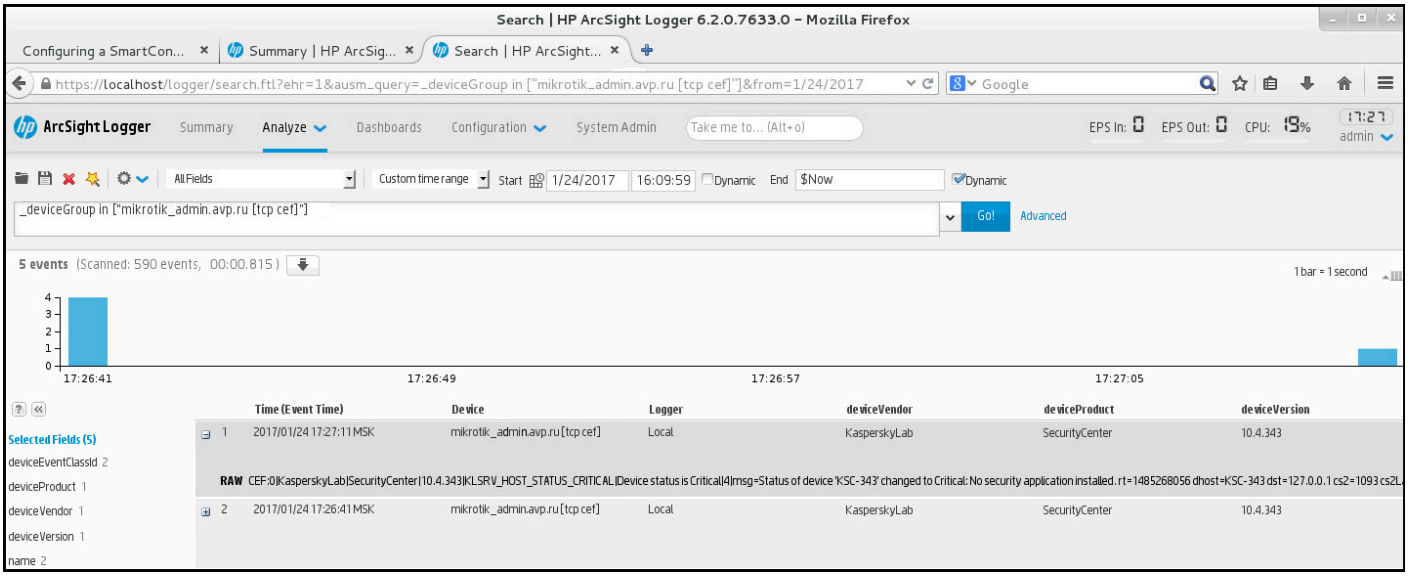
Viewing export results

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 Next Expert View are received and properly parsed by your SIEM system, configuration on both sides is done properly. Otherwise, check the settings you specified in Kaspersky Next Expert View 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

Quick Start Guide for Managed Service Providers (MSPs)

This Quick Start Guide is intended for administrators of Managed Service Providers (MSPs).

Kaspersky Next Expert View supports multitenancy. The Guide contains tips and best practices for managing accounts of your customers (tenants) and installing security applications on their devices.

About Kaspersky Next Expert View

Kaspersky Next Expert View is an application hosted and maintained by Kaspersky. You do not have to install Kaspersky Next Expert View on your computer or server. Kaspersky Next Expert View enables the administrator 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. The administrator can use a detailed dashboard that provides a snapshot of corporate device statuses, detailed reports, and granular settings in protection policies.

Key features of Kaspersky Next Expert View

Kaspersky Next Expert View enables you to do the following:

- Install Kaspersky applications on devices on your network and manage the installed applications.
- Create a hierarchy of administration groups to manage a selection of client devices as a whole.
- Create virtual Administration Servers and arrange them in a hierarchy.
- Protect your network devices, including workstations and servers:
  - Manage an antimalware protection system built on Kaspersky applications.
  - Use the detection and response (EDR and MDR) capabilities (a license for Kaspersky Endpoint Detection and Response and/or for Kaspersky Managed Detection and Response is required), including:
    - Analyzing and investigating incidents
    - Incident visualization through creating a threat development chain graph
    - Accepting or rejecting responses manually or setting up the auto-accept of all responses
- Use Kaspersky Next Expert View as a multi-tenant application.
- Remotely manage Kaspersky applications installed on client devices.
- Perform centralized deployment of license keys for Kaspersky applications to client devices.
- Create and manage security policies for devices on your network.

- Create and manage user accounts.
- Create and manage user roles (RBAC).
- Create and manage tasks for applications installed on your network devices.
- View reports on the security system status for every client organization individually.

About licensing of Kaspersky Next Expert View for MSPs

When you start using Kaspersky Next Expert View, you can either request a trial workspace (in this case, you are granted a 30-day trial license that is embedded in your workspace) or enter an activation code for a commercial license.

Later, you can add one or several commercial license keys to the Administrator Server repository.

About detection and response capabilities for MSPs

Kaspersky Next Expert View can integrate features of other Kaspersky applications into the console interface. For example, you can add the detection and response features to the functionality of Kaspersky Next Expert View by integrating the following applications:

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Detection and Response Optimum is a solution designed to protect an organization's IT infrastructure from complex cyberthreats. The solutions' functionality combines automatic threat detection with the ability to respond to these threats to resist complex attacks, including new exploits, ransomware, fileless attacks, and methods that use legitimate system tools.

  After a Kaspersky Endpoint Protection Platform (EPP) application detects a security incident, a detailed card with important data about the security incident is generated in Kaspersky Next Expert View. The incident card is generated by one of the following applications:

  - Kaspersky Endpoint Agent which is installed together with a Kaspersky EPP application
  - Kaspersky Endpoint Security 11.7.0 for Windows or later which has built-in EDR Optimum functionality and does not require additional installation of Kaspersky Endpoint Agent

  An incident card enables you to analyze and investigate the incident. Also, you can visualize the incident by creating a threat development chain graph. The graph describes the deployment stages of the detected attack in time. The created graph includes information about the modules involved in the attack and the actions performed by these modules.

  You can also initiate a chain of response actions: create an execution prevention rule for an untrusted object; search for similar incidents in the device group, based on the selected indicators of compromise (IOC); isolate an untrusted object; isolate a compromised device from the network.

  For information about the application activation, see the Kaspersky Endpoint Detection and Response Optimum documentation.

  If integrated, this application adds the **Alerts** section to the interface of Kaspersky Next Expert View (**Monitoring** → **Alerts**).

- Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response delivers round-the-clock protection from the growing volume of threats that circumvent automated security barriers to organizations who struggle to find the expertise and staff, or for those with limited in-house resources. The MDR SOC analysts of Kaspersky or a third-party company investigate the incidents and offer responses to solve the incidents. You can accept or reject the offered measures manually, or enable the option to auto-accept all of the responses.

For information about the application activation, see the Kaspersky Managed Detection and Response documentation.

If integrated, this application adds the **Incidents** section to the interface of Kaspersky Next Expert View (**Monitoring** → **Incidents**).

You can show or hide the interface elements that refer to the Kaspersky Endpoint Detection and Response or Kaspersky Managed Detection and Response features at any time in the **Interface options** section of Kaspersky Next Expert View.

Getting started with Kaspersky Next Expert View

After you complete the scenario in this section, Kaspersky Next Expert View is ready to use.

Getting started scenario

The scenario proceeds in stages:

1. **Create an account**

   To start using Kaspersky Endpoint Security Cloud, you need a Kaspersky Next Expert View user account.

   To create an account:

   1. Open your browser and enter the following address: https://cloud.kaspersky.com.
   2. Click the **Create an account** button.
   3. Follow the onscreen instructions.

2. **Create a workspace**

   After you create the account, you can create your first workspace. We recommend that you first create one test workspace, connect your own devices to it, and then test any modifications to the settings, noting the results.

   To create a workspace:

   1. Open your browser and enter the following address: https://cloud.kaspersky.com.
   2. Click the **Sign in** button.
   3. Follow the onscreen instructions.

3. **Perform initial setup of Kaspersky Next Expert View**

   When you enter the created workspace for the first time, you are automatically prompted to run the quick start wizard. The quick start wizard guides you to create a minimum of necessary tasks and policies, adjust a minimum of settings, and start creating installation packages of Kaspersky applications. Follow the onscreen instructions.

When initial setup is complete, Kaspersky Next Expert View is ready to use.

Recommendations on managing your customers' devices

This section contains recommendations for organizing the customer devices that you want to protect.

Recommendations depend on whether you are using Kaspersky Security Center for the first time or have already used the on-premises version:

- If you have never used Kaspersky Security Center before, you have two options:

  - Create a virtual Administration Server for the devices of each customer (recommended option). In this case, the devices of each customer can be managed through a dedicated virtual Administration Server independently from other customers. At the same time, you can use the primary Administration Server to create common policies and tasks for all of the customers. The reports generated on the primary Administration Server can include data from all of the virtual Administration Servers.

  - Create an administration group for the devices of each customer. If you want to divide customer devices further, you can create a hierarchy of subordinate administration groups under each parent group. For example, you may need subordinate groups if you want to use different protection settings for devices of employees who work in different departments.

- If you have already used Kaspersky Security Center running on-premises, you can migrate your existing administration groups and related objects from Kaspersky Security Center on-premises to Kaspersky Next Expert View.

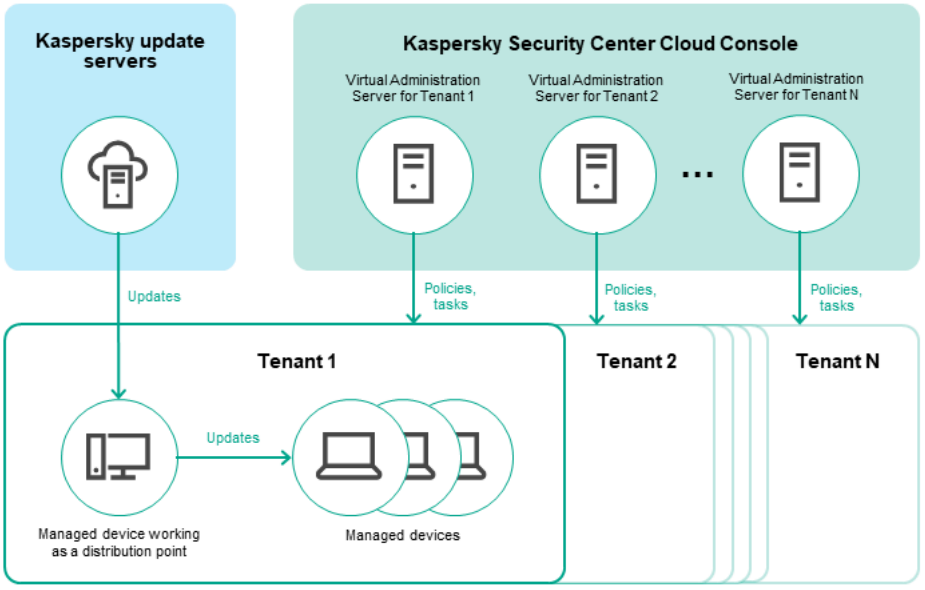
  You cannot migrate virtual Administration Servers. After migrating the administration groups and other objects, you can create virtual Administration Servers in Kaspersky Next Expert View.

  Proceed to configuring migration.

The administrator of a virtual Administration Server can only proceed to this virtual Server from the primary Administration Server. All the objects created on the primary Administration Server are available for reading to the administrator of a virtual Administration Server (for example, widgets, reports, or the user roles).

Typical deployment scheme for MSPs

This section provides a description of the deployment scheme typically used by MSPs to manage multiple tenants. The scheme is based on management through virtual Administration Servers individually created for each tenant.



Typical deployment scheme for MSPs

The scheme comprises the following main components:

- *Kaspersky Next Expert View*. Provides a user interface to the administration services of your workspace. You use Kaspersky Next Expert View to deploy, manage, and maintain the protection system of a client organization's network.
- *Kaspersky update servers*. HTTP(S) servers at Kaspersky from which Kaspersky applications download database and application module updates.
- *Virtual Administration Servers*. An MSP administrator typically creates a virtual Administration Server for each tenant to deploy, manage, and maintain the protection system of the corresponding client organization's network.
- *Tenants*. Client organizations whose devices are to be protected.
- *Managed devices*. A client company's devices protected by Kaspersky Next Expert View. Each device that has to be protected must have Network Agent and one of the Kaspersky security applications installed.
- *Managed device working as a distribution point*. Computer that has Network Agent installed and is used for update distribution, network polling, remote installation of applications, getting information about computers in an administration group, and / or broadcasting domain. The administrator selects the appropriate devices and manually assigns them as distribution points. Distribution points can also act as Connection Gateways to reduce the number of outgoing external connections and the number of simultaneous connections to the Administration Server. It is recommended to limit the number of managed computers that connect directly to the Administration Server.

Scenario: Protection deployment (tenant management through virtual Administration Servers)

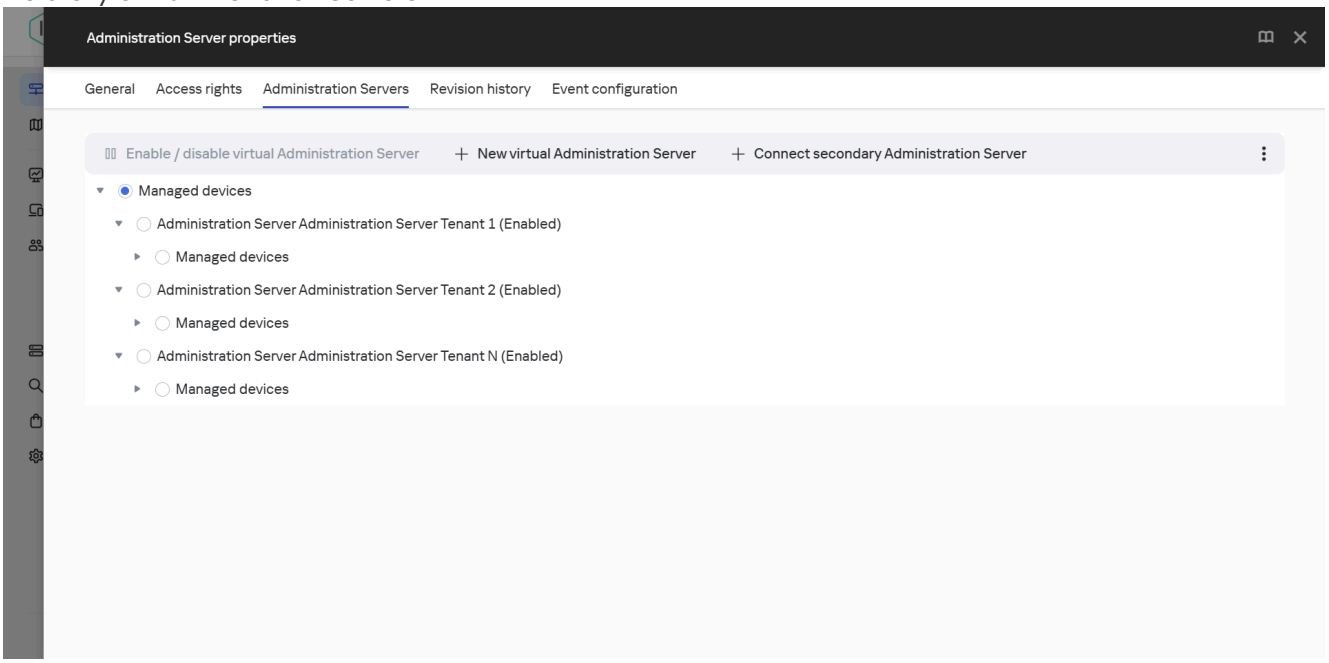
If you have never used Kaspersky Security Center and you want to manage your tenants through virtual Administration Servers, proceed as described in this section. After you complete this scenario, your customers' devices will be protected.

If you manage several tenants, then perform the scenario for each of the tenants separately.

The scenario proceeds in stages:

1. **Creating a virtual Administration Server**

   Create a virtual Administration Server for your customer. The new virtual Administration Server appears in the hierarchy of Administration Servers:



Virtual Administration Servers in the hierarchy of Administration Servers

2. **Selecting a device to act as a distribution point**

   Among the devices of the customer, decide which device will act as a distribution point.

   > You cannot have more than 100 distribution points within one workspace.

3. **Creating a stand-alone installation package for Network Agent**

   Switch to the created virtual Administration Server, and then create a stand-alone installation package for Network Agent. You can switch Administration Servers in the main menu by clicking the chevron icon (›) to the right of the current Administration Server name, and then selecting the required Administration Server. During creation of the stand-alone installation package, specify the Managed devices administration group to move the device to.

4. **Installing Network Agent on the selected device to act as a distribution point**

You can use any method that is suitable for you:

- Manual installation

  To deliver the stand-alone installation package to the device, you can, for example, copy it to a removable drive (such as a flash drive) or place it in a shared folder.

- Deployment by using Active Directory

- Deployment by using your remote monitoring and management (RMM) software solution

5. **Assigning a distribution point**

   Assign the device with Network Agent installed to act as a distribution point.

6. **Network polling**

   Configure and perform network polling through the distribution point.

   Kaspersky Next Expert View provides the following methods of network polling:

   - IP range polling
   - Windows network polling
   - Active Directory polling

   After network polling according to schedule is complete, your customers' devices are discovered and placed in the **Unassigned devices** group.

7. **Moving the discovered devices to the administration groups**

   Set up the rules for automatically moving the discovered devices to the required administration groups; or move these devices to the required administration groups manually. If you plan to manage the customer's devices in a single administration group, you can move the devices to the Managed devices group.

8. **Creating installation packages for Network Agent and managed Kaspersky applications**

   Create installation packages for Kaspersky applications.

9. **Removing third-party security applications**

   If third-party security applications are installed on your customers' devices, remove them before installing Kaspersky applications.

10. **Installing Kaspersky applications on client devices**

    Create remote installation tasks to install Network Agent and managed Kaspersky applications on your customers' devices.

    If necessary, you can create several remote installation tasks to install managed Kaspersky applications for different administration groups or different device selections.

    After the tasks are created, you can configure their settings. Make sure that the schedule for each task meets your requirements. First, the task to install Network Agent must be run. After Network Agent is installed on your customers' devices, the task to install managed Kaspersky applications must be run.

11. **Verifying initial deployment of Kaspersky applications**

    Generate and view the **Report on Kaspersky application versions**. Make sure that the managed Kaspersky applications are installed on all of the devices of your customer.

12. **Creating policies for Kaspersky applications**

    Create a policy for the required Kaspersky application. If you want to create a universal policy for all your customers, switch the current virtual Administration Server to the primary Administration Server, and then create a policy for the required Kaspersky application.

Scenario: Protection deployment (tenant management through administration groups)

If you have never used Kaspersky Security Center and you want to manage your tenants through administration groups, proceed as described in this section. After you complete this scenario, your customers' devices will be protected.

The scenario proceeds in stages:

1. **Creating administration groups**

   Create an administration group for each of your customers.

2. **Planning the distribution points structure**

   Among the devices of each customer, decide which device will act as a distribution point.

   > You cannot have more than 100 distribution points within one workspace.

3. **Creating a stand-alone installation package for Network Agent**

   Create a stand-alone installation package for Network Agent.

4. **Installation of Network Agent on the selected devices to act as distribution points**

   Install Network Agent on the selected devices that will act as distribution points.

   You can use any method that is suitable for you:

   - Manual installation

     To deliver the stand-alone installation package to the devices, you can, for example, copy it to a removable drive (such as a flash drive) or place it in a shared folder.

   - Deployment by using Active Directory

   - Deployment by using your remote monitoring and management (RMM) software solution

5. **Assigning distribution points**

   Assign the devices with Network Agent installed to act as distribution points.

6. **Network polling**

   Configure and perform network polling through the distribution point.

Kaspersky Next Expert View provides the following methods of network polling:

- IP range polling
- Windows network polling
- Active Directory polling

After network polling according to schedule is complete, your customers' devices are discovered and placed in the **Unassigned devices** group.

7. **Moving the discovered devices to the administration groups**

   Set up the rules for automatically moving the discovered devices to the required administration groups; or move these devices to the required administration groups manually.

8. **Creating installation packages for Network Agent and managed Kaspersky applications**

   If you did not start the quick start wizard, or skipped the step of creating installation packages, create installation packages for Kaspersky applications.

9. **Removing third-party security applications**

   If third-party security applications are installed on your customers' devices, remove them before installing Kaspersky applications.

10. **Installing Kaspersky applications on your customers' devices**

    Create remote installation tasks to install Network Agent and managed Kaspersky applications on your customers' devices.

    If necessary, you can create several remote installation tasks to install managed Kaspersky applications for different administration groups or different device selections.

    After the tasks are created, you can configure their settings. Make sure that the schedule for each task meets your requirements. First, the task to install Network Agent must be run. After Network Agent is installed on your customers' devices, the task to install managed Kaspersky applications must be run.

11. **Verifying initial deployment of Kaspersky applications**

    Generate and view the **Report on Kaspersky application versions**. Make sure that the managed Kaspersky applications are installed on all of the devices of your customers.

12. **Creating policies for Kaspersky applications**

    Go to the **Asset management** → **Groups** section; if you want to create a universal policy for all your customers, select **Administration Server.** If you want to create a specific policy for an individual customer, select the administration group corresponding to that customer. Create a policy for the required Kaspersky application.

Joint usage of Kaspersky Security Center on-premises and Kaspersky Next Expert View

If you have already used Kaspersky Security Center running on-premises, you can convert your existing Administration Servers running on-premises into secondary Administration Servers of your new Kaspersky Next Expert View Administration Server, as described in this section.

If you configure joint usage of Kaspersky Security Center on-premises and Kaspersky Next Expert View, you will not be able to migrate from Kaspersky Security Center on-premises to Kaspersky Next Expert View unless you remove the hierarchy of Administration Servers.

To create a hierarchy of Administration Servers,

Add your existing Administration Servers running on-premises as secondary Administration Servers.

Licensing of Kaspersky applications for MSPs

Kaspersky Next Expert View enables you to perform centralized distribution of license keys for Kaspersky applications on your customers' devices, monitor their use, and renew licenses.

If you manage several tenants, you can distribute license keys in the following ways:

- One license key for all of the tenants.
- An individual license key for each tenant.

To distribute license keys to your customers' devices:

1. Add the required license keys to the Administration Server repository.
2. Do one of the following:
   - Configure automatic distribution of a license key.

     In this case, Kaspersky Next Expert View selects one of the applicable license keys and automatically deploys it every time a new device is discovered.
   - Configure the Add a key task to distribute a license key to devices.

     When configuring the task, you select the license key that must be deployed to devices and select the administration group that contains the required devices.

     One task can distribute only one license key. This means that if you want to distribute several license keys, you must create a task for each of them.

The Kaspersky applications installed on your customers' devices are activated.

Adding an active license key to the primary Administration Server is mandatory. Otherwise, the associated workspace will be deleted in 90 days, regardless of the status of license keys on other Administration Servers within that workspace.

Monitoring and reporting capabilities for MSPs

Kaspersky Next Expert View provides you with monitoring and reporting capabilities. These capabilities give you an overview of your organization infrastructure, protection statuses, and statistics.

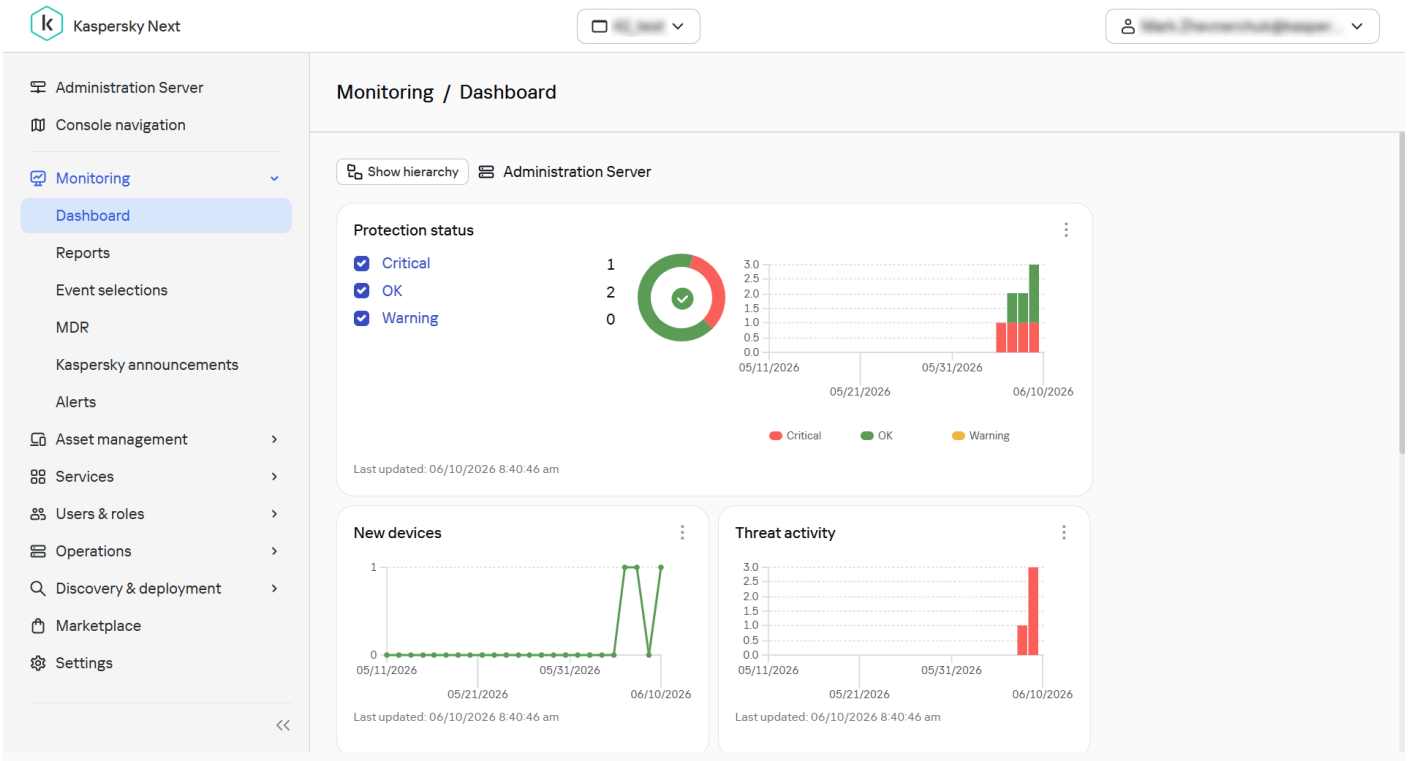
When you have deployed Kaspersky Next Expert View, you can configure the monitoring and reporting features to best suit your needs.

Kaspersky Next Expert View provides the following types features of monitoring and reporting:

- Dashboard
- Reports
- Event selections
- Email notifications

Dashboard

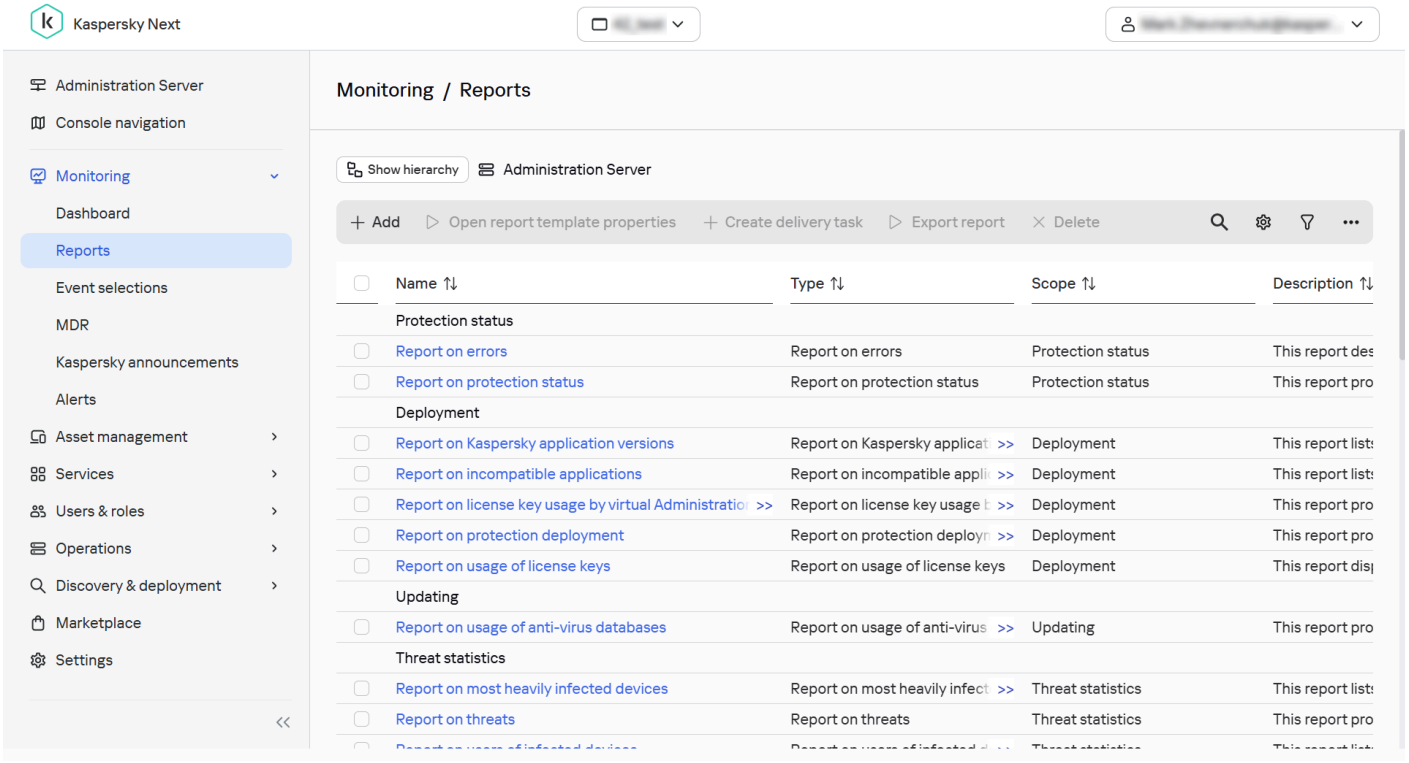
The dashboard allows you to monitor security trends on your organization's network by providing you with a graphical display of information. (See the figure below.)



The Dashboard section

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. You can also schedule report delivery by email (see the figure below).



The Reports section

Event selections

Event selections allow viewing named sets of events selected from the Administration Server database. Kaspersky Next Expert View contains some predefined event selections (for example, **Recent events** and **Critical events**). Also, you can create custom event selections.

Email notifications.

You can configure email notification about events occurring in Kaspersky Next Expert View and on your customers' devices.

Working with Kaspersky Next Expert View in a cloud environment

This section provides information about Kaspersky Next Expert View features related to the operation and maintenance of Kaspersky Next Expert View in cloud environments, such as Amazon Web Services, Microsoft Azure, or Google Cloud.

To work within a cloud environment, you need a special license. If you do not have such a license, the interface elements related to cloud devices are not operable.

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.

Licensing options in a cloud environment

Work in a cloud environment is possible both in trial mode and in commercial mode of Kaspersky Next Expert View:

- In trial mode, all cloud environment features are available within the entire validity period of your workspace. No license is required.
- In commercial mode, the cloud environment features are available only if a Kaspersky Hybrid Cloud Security license key has been added as active in the Administration Server properties.

In both cases, Vulnerability and patch management is automatically activated.

If an error occurs when trying to activate the feature Support of the cloud environment using the license for Kaspersky Hybrid Cloud Security, use the key file.

Preparing for work in a cloud environment through Kaspersky Next Expert View

This section tells you how to prepare for working with Kaspersky Next Expert View in the following cloud environments:

- Amazon Web Services
- Microsoft Azure
- Google Cloud

Working in Amazon Web Services cloud environment

This section tells you how to prepare for working with Kaspersky Next Expert View in Amazon Web Services.

The addresses of web pages cited in this document are correct as of the Kaspersky Next Expert View release date.

About work in Amazon Web Services cloud environment

To work with the AWS platform and, in particular, to create instances, you need an Amazon Web Services account. You can create a free account at https://aws.amazon.com. You can also use an existing Amazon account.

To learn more about an AMI and how AWS Marketplace works, please visit the AWS Marketplace Help page. For more information about working with the AWS platform, using instances, and related concepts, please refer to the Amazon Web Services documentation.

The addresses of web pages cited in this document are correct as of the Kaspersky Next Expert View release date.

Creating IAM user accounts for Amazon EC2 instances

This section describes the actions that must be performed to ensure correct operation of Kaspersky Next Expert View. These actions include work with the AWS Identity and Access Management (IAM) user accounts. Also described are the actions that must be taken on client devices to install Network Agent on them and then install Kaspersky Endpoint Security for Linux.

Ensuring that Kaspersky Next Expert View has the permissions to work with AWS

To operate in the Amazon Web Services cloud environment using Kaspersky Next Expert View, you must create an *IAM user account*, that will be used by Kaspersky Next Expert View to work with AWS services. Before starting to work with the Administration Server, create an IAM user account with an *AWS IAM access key* (hereinafter also referred to as *IAM access key*).

Creation of an IAM user account requires the AWS Management Console. To work with the AWS Management Console, you will need a user name and password from an account in AWS.

Creating an IAM user account for work with Kaspersky Next Expert View

An IAM user account is required for working with Kaspersky Next Expert View. You can create one IAM user account with all the necessary permissions, or you can create two separate user accounts.

An *IAM access key* that you will need to provide to Kaspersky Next Expert View during initial configuration is automatically created for the IAM user. An IAM access key consists of an access key ID and a secret key. For more details about the IAM service, please refer to the following AWS reference pages:

- https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- https://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

To create an IAM user account with the necessary permissions:

1. Open the AWS Management Console and sign in under your account.
2. In the list of AWS services, select **IAM**.

   A window opens containing a list of user names and a menu that lets you work with the tool.
3. Navigate through the areas of the console dealing with user accounts, and add a new user name or names.
4. For the user(s) you add, specify the following AWS properties:
   - Access type: **Programmatic Access**.
   - Permissions boundary not set.
   - Permission: **ReadOnlyAccess**.

     After you add the permission, view it for accuracy. In case of a mistaken selection, go back to the previous screen and make the selection again.
5. After you create the user account, a table appears containing the IAM access key of the new IAM user. The access key ID is displayed in the **Access key ID** column. The secret key is displayed as asterisks in the **Secret access key** column. To view the secret key, click **Show**.

The newly created account is displayed in the list of IAM user accounts that corresponds to your account in AWS.

The addresses of web pages cited in this document are correct as of the Kaspersky Next Expert View release date.

Working in Microsoft Azure cloud environment

This section provides information about Kaspersky Next Expert View operation and maintenance in a cloud environment provided by Microsoft Azure, as well as details of protection deployment on virtual machines in this cloud environment.

About work in Microsoft Azure

To work with the Microsoft Azure platform and, in particular, to purchase apps at the Azure Marketplace and create virtual machines, you will need an Azure subscription. Before starting to work with Microsoft Azure in Kaspersky Next Expert View, create an Azure Application ID with permissions required for installation of applications on virtual machines.

Creating a subscription, Application ID, and password

To work with Kaspersky Next Expert View in the Microsoft Azure environment, you need an Azure subscription, Azure Application ID, and Azure Application password. You can use an existing subscription, if you already have one.

An Azure subscription grants its owner access to the Microsoft Azure Platform Management Portal and to Microsoft Azure services. The owner can use the Microsoft Azure Platform to manage services such as Azure SQL and Azure Storage.

To create a Microsoft Azure subscription,

Go to https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription and follow the instructions there.

More information about creating a subscription is available on the Microsoft website. You will get a subscription ID, which you will later provide to Kaspersky Next Expert View together with Application ID and password.

To create and save Azure Application ID and password:

1. Go to https://portal.azure.com and make sure that you are logged in.
2. Following the instructions on the reference page, create your Application ID.
3. Go to the **Keys** section of the application settings.
4. In the **Keys** section, fill in the **Description** and **Expires** fields and leave the **Value** field empty.
5. Click the **Save** button.

   When you click **Save**, the system automatically fills the **Value** field with a long sequence of characters. This sequence is your Azure Application password (for example, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QIfFvdU=). The description is displayed as you entered it.
6. Copy the password and save it, so that you can later provide the Application ID and password to Kaspersky Next Expert View.

   You can copy the password only when it has been created. Later, the password will no longer be displayed and you cannot restore it.

The addresses of web pages cited in this document are correct as of the Kaspersky Next Expert View release date.

Assigning a role to the Azure Application ID

If you only want to detect virtual machines using device discovery, your Azure Application ID must have the Reader role. If you want not only to detect virtual machines, but also to deploy protection by means of the Azure API, your Azure Application ID must have the Virtual Machine Contributor role.

Follow the instructions on the Microsoft website to assign a role to your Azure Application ID.

Working in Google Cloud

This section provides information about work with Kaspersky Next Expert View in a cloud environment provided by Google.

You can use the Google API to work with Kaspersky Next Expert View in Google Cloud Platform. A Google account is required. Please refer to the Google documentation at https://cloud.google.com for more information.

You will need to create and provide Kaspersky Next Expert View with the following credentials:

- **Client email**

  Client email is the email address that you used for registering your project at Google Cloud.

- **Project ID**

  Project ID is the ID that you received when you registered your project at Google Cloud.

- **Private key**

  Private key is the sequence of characters that you received as your private key when you registered your project at Google Cloud. You might want to copy and paste this sequence to avoid mistakes.

Cloud environment configuration wizard in Kaspersky Next Expert View

To configure Kaspersky Next Expert View using this wizard, you must have the following:

- Specific credentials for a cloud environment:
  - An IAM user account that has been granted the right to poll the cloud segment (for work with Amazon Web Services)
  - Azure Application ID, password, and subscription (for work with Microsoft Azure)
  - Google client email, Project ID, and private key (for work with Google Cloud)
- Installation packages:
  - Network Agent for Windows
  - Network Agent for Linux
  - Kaspersky Endpoint Security for Linux
- Web plug-in for Kaspersky Endpoint Security for Linux

- At least one of the following:
  - Installation package and web plug-in for Kaspersky Endpoint Security for Windows (recommended)
  - Installation package and web plug-in for Kaspersky Security for Windows or Linux Server

If your workspace was created by using the Kaspersky Hybrid Cloud Security license, the Cloud environment configuration wizard starts automatically at the first connection to Kaspersky Next Expert View. If you skip the Cloud environment configuration wizard, it will start at every connection to Kaspersky Next Expert View until you finish all the steps of the wizard.

You can also start the Cloud environment configuration wizard manually at any time.

To start the Cloud environment configuration wizard manually,

In the main menu, go to **Discovery & deployment** → **Deployment & assignment** → **Configure cloud environment**.

The wizard starts.

An average work session with this wizard lasts about 15 minutes.

If you did not activate Administration Server under the Kaspersky Hybrid Cloud Security license, you have to do it at the initial step of the wizard.

Step 1. Checking the required plug-ins and installation packages

This step is not displayed if you have all of the required web plug-ins and installation packages listed below.

To configure a cloud environment, you must have the following components:

- Installation packages:
  - Network Agent for Windows
  - Network Agent for Linux
  - Kaspersky Endpoint Security for Linux
- Web plug-in for Kaspersky Endpoint Security for Linux
- Installation package and web plug-in for Kaspersky Endpoint Security for Windows

Kaspersky Next Expert View automatically detects the components that you already have and lists only ones that are missing. Download the listed components by clicking the **Select applications to download** button, and then selecting the required plug-ins and installation packages. After you download a component, you can use the **Refresh** button to update the list of missing components.

Step 2. Selecting the application activation method

This step is displayed only if you used a license other than Kaspersky Hybrid Cloud Security during the workspace creation and never added a Kaspersky Hybrid Cloud Security license key to the activation field of Administration Server. In this case, you must activate Administration Server by using a Kaspersky Hybrid Cloud Security license.

Step 3. Selecting the cloud environment and authorization

Specify the following settings:

- **Cloud environment**

  Select the cloud environment in which you are deploying Kaspersky Next Expert View: AWS, Azure, or Google Cloud.

  If you plan to work with more than one cloud environment, select one environment and then run the wizard again.

- **Connection name**

  Enter a name for the connection. The name cannot contain more than 256 characters. Only Unicode characters are permitted.

  This name will also be used as the name for the administration group for the cloud devices.

  If you plan to work with more than one cloud environment, you might want to include the name of the environment in the connection name, for example, "Azure Segment", "AWS Segment", or "Google Segment".

Enter your credentials to receive authorization in the cloud environment that you specified.

AWS

If you selected AWS as the cloud segment type, use an AWS IAM access key for further polling of the cloud segment. Enter the following key data:

- **Access key ID**

  The IAM access key ID is a sequence of alphanumeric characters. You received the key ID when you created the IAM user account.

  The field is available after you selected an AWS IAM access key for authorization.

- **Secret key**

  The secret key that you received with the access key ID when you created the IAM user account.

  The characters of the secret key are displayed as asterisks. After you begin entering the secret key, the **Show** button is displayed. Click and hold this button for the necessary amount of time to view the characters you entered.

  The field is available after you selected an AWS IAM access key for authorization.

  To see the characters that you entered, click and hold the **Show** button.

Azure

If you selected Azure as the cloud segment type, specify the following settings for the connection that will be used for further polling of the cloud segment:

- **Azure Application ID**

  You created this application ID on the Azure portal.

  You can provide only one Azure Application ID for polling and other purposes. If you want to poll another Azure segment, you must first delete the existing Azure connection.

- **Azure Subscription ID**

  You created the subscription on the Azure portal.

- **Azure Application password**

  You received the password of the Application ID when you created the Application ID.

  The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.

  To see the characters that you entered, click and hold the **Show** button.

- **Azure storage account name**

  You created the name of the Azure storage account for working with Kaspersky Next Expert View.

- **Azure storage access key**

  You received a password (key) when you created Azure storage account for working with Kaspersky Next Expert View.

  The key is available in section "Overview of the Azure storage account", in subsection "Keys".

  To see the characters that you entered, click and hold the **Show** button.

Google Cloud

If you selected Google Cloud as the cloud segment type, specify the following settings for the connection that will be used for further polling the cloud segment:

- **Client email address**

  Client email is the email address that you used for registering your project at Google Cloud.

- **Project ID**

  Project ID is the ID that you received when you registered your project at Google Cloud.

- **Private key**

  Private key is the sequence of characters that you received as your private key when you registered your project at Google Cloud. You might want to copy and paste this sequence to avoid mistakes.

To see the characters that you entered, click and hold the **Show** button.

The connection that you specified is saved in the application settings.

The Cloud environment configuration wizard enables you to specify only one segment. Later, you can specify more connections to manage other cloud segments.

Click **Next** to proceed.

Step 4. Segment polling and configuring synchronization with Cloud

At this step, cloud segment polling starts and a special administration group for cloud devices is automatically created. The devices found during polling are placed into this group. The cloud segment polling schedule is configured every five minutes by default (you can change this setting later).

A **Synchronize with Cloud** automatic moving rule is also created. For each subsequent scan of the cloud network, virtual devices that are detected will be moved to the corresponding subgroup within the **Managed devices\Cloud** group.

Manage the **Synchronize administration groups with cloud structure** setting.

If this option is enabled, the **Cloud** group is automatically created within the **Managed devices** group and a cloud device discovery is started. The instances and virtual machines detected during each cloud network scan are placed into the Cloud group. The structure of the administration subgroups within this group matches the structure of your cloud segment (in AWS, availability zones and placement groups are not represented in the structure; in Azure, subnets are not represented in the structure). Devices that have not been identified as instances in the cloud environment are in the **Unassigned devices** group. This group structure enables you to use group installation tasks to install anti-virus applications on instances, as well as set up different policies for different groups.

If this option is disabled, the **Cloud** group is also created and the cloud device discovery is also started; however, subgroups matching the cloud segment structure are not created within the group. All detected instances are in the **Cloud** administration group so they are displayed in a single list. If your work with Kaspersky Next Expert View requires synchronization, you can modify the properties of the **Synchronize with Cloud** rule and enforce it. Enforcing this rule alters the structure of subgroups in the Cloud group so that it matches the structure of your cloud segment.

By default, this option is disabled.

Click **Next** to proceed.

Step 5. Configuring Kaspersky Security Network for Kaspersky Next Expert View

This step is skipped when running Kaspersky Next Expert View in trial mode or on a virtual Administration Server.

Specify the settings for relaying information about Kaspersky Next Expert View operations to the Kaspersky Security Network (KSN) knowledge base. Choose one of the following options:

- **I agree to participate in Kaspersky Security Network**

  Kaspersky Next Expert View 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 Next Expert View 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.

Kaspersky recommends participation in Kaspersky Security Network.

KSN agreements for managed applications may also be displayed. If you agree to use Kaspersky Security Network, the managed application will send data to Kaspersky. If you do not agree to participate in Kaspersky Security Network, the managed application will not send data to Kaspersky. You can change this setting later in the application policy.

Click **Next** to proceed.

Step 6. Creating an initial configuration of protection

You can check a list of policies and tasks that are created.

Wait for the creation of policies and tasks to complete, and then click **Next** to proceed. On the last page of the wizard, click the **Finish** button to exit.

Network segment polling via Kaspersky Next Expert View

Information about the structure of the network (and devices in it) is received through regular polling of cloud segments by using the AWS API, Azure API, or Google API tools. Kaspersky Next Expert View uses this information to update the contents of the Unassigned devices and Managed devices folders. If you have configured devices to be moved to administration groups automatically, detected devices are included in administration groups.

To allow the polling of cloud segments, you must have the corresponding rights that are provided with an IAM user account (in AWS); with an Application ID and password (in Azure); or with a Google client email, Google project ID, and private key (in Google Cloud).

You can add and delete connections, as well as set the polling schedule, for each cloud segment.

Adding connections for cloud segment polling via Kaspersky Next Expert View

To add a connection for cloud segment polling to the list of available connections:

1. In the main menu, go to **Discovery & deployment** → **Discovery** → **Cloud**.
2. In the window that opens, click **Properties**.
3. In the **Settings** window that opens, click **Add**.

   The **Cloud segment settings** window opens.
4. Specify the name of the cloud environment for the connection that will be used for further polling of the cloud segment:

   - **Cloud environment**

     Select the cloud environment in which you are deploying Kaspersky Next Expert View: AWS, Azure, or Google Cloud.

     If you plan to work with more than one cloud environment, select one environment and then run the wizard again.

   - **Connection name**

     Enter a name for the connection. The name cannot contain more than 256 characters. Only Unicode characters are permitted.

     This name will also be used as the name for the administration group for the cloud devices.

     If you plan to work with more than one cloud environment, you might want to include the name of the environment in the connection name, for example, "Azure Segment", "AWS Segment", or "Google Segment".
5. Enter your credentials to receive authorization in the cloud environment that you specified.

   - If you selected AWS, specify the following:

     - **Access key ID**

       The IAM access key ID is a sequence of alphanumeric characters. You received the key ID when you created the IAM user account.

       The field is available after you selected an AWS IAM access key for authorization.

     - **Secret key**

       The secret key that you received with the access key ID when you created the IAM user account.

       The characters of the secret key are displayed as asterisks. After you begin entering the secret key, the **Show** button is displayed. Click and hold this button for the necessary amount of time to view the characters you entered.

       The field is available after you selected an AWS IAM access key for authorization.

       To see the characters that you entered, click and hold the **Show** button.

- If you selected Azure, specify the following settings:

  - **Azure Application ID**

    You created this application ID on the Azure portal.

    You can provide only one Azure Application ID for polling and other purposes. If you want to poll another Azure segment, you must first delete the existing Azure connection.

  - **Azure Subscription ID**

    You created the subscription on the Azure portal.

  - **Azure Application password**

    You received the password of the Application ID when you created the Application ID.

    The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.

    To see the characters that you entered, click and hold the **Show** button.

  - **Azure storage account name**

    You created the name of the Azure storage account for working with Kaspersky Next Expert View.

  - **Azure storage access key**

    You received a password (key) when you created Azure storage account for working with Kaspersky Next Expert View.

    The key is available in section "Overview of the Azure storage account", in subsection "Keys".

    To see the characters that you entered, click and hold the **Show** button.

If you selected Google Cloud, specify the following settings:

- **Client email address**

  Client email is the email address that you used for registering your project at Google Cloud.

- **Project ID**

  Project ID is the ID that you received when you registered your project at Google Cloud.

- **Private key**

  Private key is the sequence of characters that you received as your private key when you registered your project at Google Cloud. You might want to copy and paste this sequence to avoid mistakes.

  To see the characters that you entered, click and hold the **Show** button.

6. If you want, click **Set polling schedule** and change the default settings.

The connection is saved in the application settings.

After the new cloud segment is polled for the first time, the subgroup corresponding to that segment appears in the **Managed devices\Cloud** administration group.

If you specify incorrect credentials, no instances will be found during cloud segment polling and a new subgroup will not appear in the **Managed devices\Cloud** administration group.

Deleting a connection for cloud segment polling

If you no longer have to poll a specific cloud segment, you can delete the connection corresponding to it from the list of available connections. You can also delete a connection if, for example, permissions to poll a cloud segment have been transferred to another user who has different credentials.

To delete a connection:

1. In the main menu, go to **Discovery & deployment → Discovery → Cloud**.
2. In the window that opens, click **Properties**.
3. In the **Settings** window that opens, click the name of the segment that you want to delete.
4. Click the **Delete** button.
5. In the window that opens, click **OK** to confirm your selection.

   The connection is deleted. The devices in the cloud segment corresponding to this connection are automatically deleted from the administration groups.

Configuring the polling schedule via Kaspersky Next Expert View

Cloud segment polling is performed according to schedule. You can set the polling frequency.

The polling frequency is automatically set at five minutes by the Cloud environment configuration wizard. You can change this value at any time and set a different schedule. However, it is not recommended to configure polling to run more frequently than every five minutes, because this could lead to errors in the API operation.

To configure a cloud segment polling schedule:

1. In the main menu, go to **Discovery & deployment → Discovery → Cloud**.
2. In the window that opens, click **Properties**.
3. In the **Settings** window that opens, click the name of the segment for which you want to configure a polling schedule.

   The **Cloud segment settings** window opens.
4. In the **Cloud segment settings** window, click the **Set polling schedule** button.

   The **Schedule** window opens.

5. In the **Schedule** window, define the following settings:

- **Scheduled start**

  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 default, the polling runs every five minutes, starting from the current system time.

  - **By days of week**

    The polling runs regularly, on the specified days of week, and at the specified time.

    By default, the polling runs every Friday at 6:00:00 PM.

  - **Every month on specified days of selected weeks**

    The polling runs regularly, on the specified days of each month, and at the specified time.

    By default, no days of month are selected; the default start time is 6:00:00 PM.

- **Start interval (days)**

  Specify what N is equal to (for minutes or days).

- **Starting from**

  Specify when to start the first poll.

- **Run missed tasks**

  If your workspace is unavailable during the time for which the poll is scheduled, Kaspersky Next Expert View can either start the poll immediately after the workspace is available again, or wait for the next time for which the poll is scheduled.

  If this option is enabled, Kaspersky Next Expert View starts polling immediately after the workspace is available again.

  If this option is disabled, Kaspersky Next Expert View waits for the next time for which the polling is scheduled.

  By default, this option is enabled.

6. Click the **Save** button to save the settings.

The polling schedule for the segment is configured and saved.

Viewing the results of cloud segment polling via Kaspersky Next Expert View

You can view the results of cloud segment polling, that is, view the list of cloud devices managed by the Administration Server.

To view the results of cloud segment polling,

In the main menu, go to **Discovery & deployment → Discovery → Cloud**.

The cloud segments available for polling are displayed.

Viewing the properties of cloud devices via Kaspersky Next Expert View

You can view the properties of each cloud device.

To view the properties of a cloud device:

1. In the main menu, go to **Asset management → Assets (Devices)**.
2. Click the name of the device whose properties you want to view.

   A property window opens with the **General** section selected.
3. If you want to view the properties specific for cloud devices, select the **System** section in the properties window.

   The properties are displayed depending on the cloud platform of the device.

   For devices in AWS, the following properties are displayed:

   - **Device discovered using API** (value: **AWS**)
   - **Cloud region**
   - **Cloud VPC**
   - **Cloud availability zone**
   - **Cloud subnet**
   - **Cloud placement group** (this unit is only displayed if the instance belongs to a placement group; otherwise, it is not displayed)

   For devices in Azure, the following properties are displayed:

   - **Device discovered using API** (value: **Microsoft Azure**)
   - **Cloud region**
   - **Cloud subnet**

   For devices in Google Cloud, the following properties are displayed:

   - **Device discovered using API** (value: **Google Cloud**)
   - **Cloud region**
   - **Cloud VPC**

- **Cloud availability zone**
- **Cloud subnet**

Synchronization with Cloud: Configuring the moving rule

During the Cloud environment configuration wizard operation, the Synchronize with Cloud rule is created automatically. This rule enables you to automatically move devices detected in each poll from the Unassigned devices group to the Managed devices\Cloud group, to make these devices available for centralized management. By default, the rule is active after it is created. You can disable, modify, or enforce the rule at any time.

To edit the properties of the Synchronize with Cloud rule and/or enforce the rule:

1. In the main menu, go to **Discovery & deployment → Deployment & assignment → Moving rules**.

   A list of moving rules opens.

2. In the list of moving rules, select **Synchronize with cloud**.

   The rule properties window opens.

3. If necessary, specify the following settings in the **Rule conditions** tab, in the **Cloud segments** tab:

   - **Device is in a cloud segment**

     If this check box is selected, the rule is applied only to devices from the selected segment.

     If the check box is cleared, the rule is applied to devices discovered by polling the network.

     By default, this check box is enabled.

   - **Include child objects**

     If this check box is selected, the rule applies to all devices in the selected segment and in all nested cloud subsections.

     If this check box is selected, the rule is applied only to devices from the root segment.

     By default, this check box is enabled.

   - **Move devices from nested objects to corresponding subgroups**

     If this option is enabled, devices from nested objects are automatically moved to the subgroups that correspond to their structure.

     If this option is disabled, devices from nested objects are automatically moved to the root of the AWS subgroup without any further branching.

     By default, this check box is enabled.

   - **Create subgroups corresponding to containers of newly detected devices**

     If this check box is selected, when the structure of the AWS group has no subgroup that would match the section containing the device, Kaspersky Security Center creates such a subgroup.

     If the check box is cleared, a new subgroup is not created.

     By default, this check box is enabled.

- **Delete subgroups for which no match is found in the cloud segments**

  If this option is enabled, the application deletes from the AWS group all the subgroups that do not match any existing cloud objects.

  If the check box is cleared, subgroups that do not correspond to cloud objects are not deleted.

  By default, this check box is enabled.

If you enabled the **Synchronize administration groups with cloud structure** option when using the Cloud environment configuration wizard, the **Synchronize with cloud** rule is created with the **Create subgroups corresponding to containers of newly detected devices** and **Delete subgroups for which no match is found in the cloud segments** options enabled.

If you have not enabled the **Synchronize administration groups with cloud structure** setting, the **Synchronize with cloud** rule is created with these settings disabled (the check boxes are cleared). If your work with Kaspersky Next Expert View requires that the structure of subgroups in the **Managed devices****Cloud** subgroup matches the structure of cloud segments, enable the **Create subgroups corresponding to containers of newly detected devices** and **Delete subgroups for which no match is found in the cloud segments** options in the rule properties, and then enforce the rule.

4. In the **Device discovered by using the API** drop-down list, select one of the following values:

   - **No**. The device cannot be detected by using the AWS, Azure, or Google API, that is, it is either outside the cloud environment, or it is in the cloud environment but for some reason it cannot be detected by using an API.
   - **AWS**. The device is discovered by using AWS API, that is, the device definitely is in the AWS cloud environment.
   - **Azure**. The device is discovered by using Azure API, that is, the device definitely is in the Azure cloud environment.
   - **Google Cloud**. The device is discovered by using the Google API, that is, the device is definitely in the Google cloud environment.
   - No value. This criterion cannot be applied.

5. If necessary, set up other rule properties in the other sections.

The moving rule is configured.

Remote installation of applications to the Azure virtual machines

You must have a valid license to install applications on Microsoft Azure virtual machines.

Kaspersky Next Expert View supports the following scenarios:

- A client device is discovered by means of Azure API; the installation is also performed by means of an API. Using the Azure API means that you can only install the following applications:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
- A client device is discovered by means of Azure API; the installation is performed by means of a distribution point or, if there are no distribution points, manually by using standalone installation packages. You can install any application supported by Kaspersky Next Expert View in this way.

To create a task for remote installation of an application on Azure virtual machines:

1. In the main menu, go to **Asset management** → **Tasks**.
2. Click **Add**.

   The New task wizard starts.
3. Follow the steps of the wizard.
   a. Select **Install application remotely** as the task type.
   b. On the **Installation packages** page, select **Remote installation by Microsoft Azure API**.
   c. When selecting the account to access devices, use an existing Azure account, or click **Add** and enter the credentials of your Azure account:
      - **Azure Account Name**

        Enter any name for the credentials you are specifying. This name will be displayed in the list of the accounts to run the task.
      - **Azure Application ID**

        You created this application ID on the Azure portal.

        You can provide only one Azure Application ID for polling and other purposes. If you want to poll another Azure segment, you must first delete the existing Azure connection.
      - **Azure Application password**

        You received the password of the Application ID when you created the Application ID.

        The characters of the password are displayed as asterisks. After you begin entering the password, the **Show** button becomes available. Click and hold this button to view the characters you entered.
   d. Select the relevant devices from the **Managed devices\Cloud** group.

After the wizard finishes, the task for remote installation of the application appears in the list of tasks.

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 Next Expert View, we recommend contacting Technical Support. Technical Support specialists will answer all your questions about installing and using Kaspersky Next Expert View.

Kaspersky provides support of Kaspersky Next Expert View 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.

Information required for Kaspersky Technical Support specialists

When you contact Kaspersky Technical Support specialists, they may ask you to provide the following information:

- General information about Kaspersky Next Expert View
- Workspace ID
- License information
- Number of installed applications
- Tenant ID and status

You can find this information in Web Console by clicking your account name and selecting the **Support** button in the drop-down list. The **General** tab contains information about your workspace, license details, and installed applications. Copy and share this information with Kaspersky Technical Support specialists to get help on your issue.

Advanced cloud protection solutions

Kaspersky offers advanced cloud protection solutions for your infrastructure. Depending on your needs and the size of your infrastructure, you can choose one of the following solutions:

- Kaspersky Next XDR Expert Cloud. This solution combines tools for detecting and investigating advanced threats involving attacks on endpoints and lets you respond manually or automatically to detected threats.

  By using Kaspersky Next XDR Expert Cloud you can:

  - Perform Threat Hunting by creating queries to search for threats and investigate events.
  - Manage alerts by viewing information about detected indicators of attacks and intrusions into the corporate IT infrastructure.
  - Investigate incidents by managing security incidents and investigating detections.
  - Configure detection rules by creating custom correlation rules, IOC and YARA rules for detecting indicators of attack and indicators of compromise.
  - Respond to detections by performing response actions using the details of an alert, incident, event, or device.
  - Automate response by configuring playbooks of automatic response actions.

  For detailed information on the functionality of the solution and how to use it, see the Kaspersky Next XDR Expert Cloud Help.

- Kaspersky EDR Expert Cloud. The solution lets you proactively search for threats on endpoint devices, analyze related events, investigate incidents and respond to threats by performing response actions.

  By using Kaspersky EDR Expert Cloud you can:

  - Perform Threat Hunting by creating queries to search for threats and investigate events.
  - Manage alerts by viewing information about detected indicators of attacks and intrusions into the corporate IT infrastructure.
  - Investigate incidents by managing security incidents and investigating detections.
  - Configure detection rules by creating custom correlation rules, IOC and YARA rules for detecting indicators of attack and indicators of compromise.
  - Respond to detections by performing response actions using the details of an alert, incident, event, or device.

  For detailed information on the functionality of the solution and how to use it, see the Kaspersky EDR Expert Cloud Help.

- Kaspersky SIEM Cloud. The solution gets data from third-party event sources and analyzes it using correlation rules. You can use the obtained data for Threat Hunting, alert analysis, and incident investigation.

By using Kaspersky SIEM Cloud you can:

- Perform Threat Hunting by creating queries to search for threats and investigate events.
- Manage alerts by viewing information about detected indicators of attacks and intrusions into the corporate IT infrastructure.
- Investigate incidents by managing security incidents and investigating detections.

For detailed information on the functionality of the solution and how to use it, see the Kaspersky SIEM Cloud Help.

To find and purchase a Kaspersky advanced cloud protection solution:

1. In the main menu, go to the **Marketplace** section.
2. Select the **Cloud** asset type.

   The section displays all available Kaspersky cloud solutions.
3. Click the solution that you want to purchase or you want to learn more about.
4. You will be redirected to the solution webpage. You can follow the on-screen instructions to proceed to the purchase.

Sources of information about the application

Kaspersky Next Expert View page on the Kaspersky website

On the Kaspersky Next Expert View page on the Kaspersky website, you can view general information about the application, its functions, and features.

Kaspersky Next Expert View page in the Knowledge Base

The *Knowledge Base* is a section on the Kaspersky Technical Support website.

On the Kaspersky Next Expert View 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 Next Expert View 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.

Known issues and limitations

Kaspersky Next Expert View has a number of limitations that are not critical to operation of the application:

- Switching from Expert View to Pro View is not available now.
- At the last step of switching from Pro View to Expert View mode, the page in the new mode may not load. Refresh the page to make it display correctly.
- Notification center may not display disk encryption fault notifications for the device.
- When you add a user from the primary Administration Server to a virtual Administration Server, the user is automatically assigned the Main Administrator role.

  If you want to assign custom rights to a user (for example, to grant only the **Read** rights), go to the **Administration Server properties**. On the **Access rights** tab, select users and a virtual Administration Server, and then skip the role assignment step. The users are added to the virtual Administration Server, but they do not have any rights on this server. To assign custom right to a user, go to the virtual Administration Server properties, select the users, and then assign them custom rights.
- In **Asset management** → **Tasks**, when you select the filter in the **Task type** column, the drop-down list may display one incorrect value.
- The policy list is displayed incorrectly when the browser window is resized.
- Grouping by applications is not enabled by default in the **Policies** and **Tasks** sections.
- When switching from Pro View to Expert View repeatedly, policies for managed applications are created with duplicate names.
- Information about managed application components is not available if Network Agent is installed on Windows XP.
- You cannot add an installation package with the same localization language several times. For example, if you already added the Kaspersky Endpoint Security for Windows (English) installation package, you can add Kaspersky Endpoint Security for Windows installation packages localized in other languages, except English.
- In the **Alert details** window, if you click any link that opens another section, and then try to return and click the **Back** button of your browser (or press **`Alt`**+**`Left`**), the **Alert details** window loads indefinitely.
- In Simplified Chinese localization, information in the **Monitoring** → **MDR**, **Settings** → **Integration** → **Kaspersky EDR Expert** and **Asset management** → **Mobile devices** sections may display incorrectly.
- 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.
- If you make an attempt to log in to Kaspersky Next Expert View by using Active Directory Federation Services (AD FS), but the required permissions are missing, Kaspersky Next Expert View still returns the "Invalid credentials" error instead of warning the user of missing permissions.
- The Manage devices task does not work correctly for devices running macOS.

- In the Remote diagnostics window, clicking the **Download entire file** button might not result in correct downloading.

- An ignored third-party vulnerability (not including Microsoft software) is not shown on **the Statistics of vulnerability on devices diagram**.

Glossary

Active key

A key that is currently used by the application.

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.

Amazon EC2 instance

A virtual machine created based on an AMI image using Amazon Web Services.

AMI

The template containing the software configuration necessary for running the virtual machine. Multiple instances can be created based on a single AMI.

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 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 tag

A label for third-party applications that can be used for grouping or finding applications. A tag assigned to applications can serve as a condition in device selections.

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.

AWS Application Program Interface (AWS API)

The application programming interface of the AWS platform that is used by Kaspersky Next Expert View. Specifically, AWS API tools are used for cloud segment polling and installing Network Agent on instances.

AWS Console

The web interface for managing Amazon EC2 instances. AWS Management Console is available on the web at https://aws.amazon.com/console/.

AWS IAM access key

A combination consisting of the key ID (which looks like "AKIAIOSFODNN7EXAMPLE") and secret key (which looks like "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). This pair belongs to the IAM user and is used to obtain access to AWS services.

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 Next Expert View.

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*.

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.

Device tag

A label of a device that can be used for grouping, describing, or finding devices.

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 Next Expert View.

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.

Forced installation

Method for remote installation of Kaspersky applications that allows you to install software on specific client devices. For successful forced installation, the account used for the task must have sufficient rights to start applications remotely on client devices. This method is recommended for installing applications on devices that are running Microsoft Windows NT / 2000 / 2003 / XP operating systems and that support this functionality.

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.

IAM role

Set of rights for making requests to AWS-based services. IAM roles are not linked to a specific user or group; they provide access rights without AWS IAM access keys. You can assign an IAM role to IAM users, EC2 instances, and AWS-based applications or services.

IAM user

The user of AWS services. An IAM user may have the rights to perform cloud segment polling.

Identity and Access Management (IAM)

The AWS service that enables management of user access to other AWS services and resources.

Incompatible application

An anti-virus application from a third-party developer or a Kaspersky application that does not support management through Kaspersky Next Expert View.

Installation package

A set of files created for remote installation of a Kaspersky application by using the Kaspersky Next Expert View 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.

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 Next Expert View

An application designed for the centralized execution of basic administration and maintenance tasks on an organization's network. Kaspersky Next Expert View is hosted and maintained by Kaspersky. The application is a part of the Kaspersky Next cloud solution. Within this solution, you can also use Kaspersky Next Pro View.

Kaspersky Next Expert View account

Account required for configuring Kaspersky Next Expert View by adding or deleting user accounts and configuring security profiles (security policies). This account lets you use the My Kaspersky service. This account is created when you start using Kaspersky Next Expert View.

Kaspersky Next Expert View Administrator

The person managing application operations through the Kaspersky Next Expert View remote centralized administration system.

Kaspersky Next Expert View Operator

A user who monitors the status and operation of a protection system managed with Kaspersky Next Expert View.

Kaspersky Security Network (KSN)

An infrastructure of cloud services that provides access to the continuously updated Kaspersky knowledge base with 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.

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 device

A device with an installed security application connected to Kaspersky Next Expert View.

Management web plug-in

A special component that is used for remote administration of Kaspersky software by means of Kaspersky Next Expert View. A management plug-in is an interface between Kaspersky Next Expert View and a specific Kaspersky application. With a management plug-in, you can configure tasks and policies for the application.

Network Agent

A Kaspersky Next Expert View 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.

Policy profile

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.

Protection status

Current protection status, which reflects the protection level of the device.

Push server

A distribution point function that enables you to maintain a permanent connection between managed devices and Administration Server. This is necessary for obtaining information from the devices and for immediate execution of management commands.

Quarantine

The folder into which the Kaspersky application moves detected probably infected objects. Quarantined objects are stored encrypted to prevent them from affecting the computer.

Remote installation

Installation of Kaspersky applications by using the services provided by Kaspersky Next Expert View.

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.

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.

UEFI protection device

A device with the Kaspersky Anti-Virus for UEFI software built in at the BIOS level. Integrated protection ensures device security from the moment the system starts, while protection on devices without integrated software begins functioning only after the protection application starts.

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 Next Expert View, 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 Servers can work only as secondary Administration Servers.
- Virtual Server does not support creation of secondary Administration Servers (including virtual Servers).

Virus activity threshold

Maximum allowed number of events of the specified type within a limited time; when this number is exceeded, it is interpreted as increased virus activity and as a threat of a virus outbreak. This feature is important during periods of virus outbreaks because it enables administrators to respond in a timely manner to virus attack threats.

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.

Work area

Virtual administration server by Kaspersky for managing security applications on devices connected to Kaspersky Next Expert View, as well as for storing individual settings of Kaspersky Next Expert View and registration information of the company that uses this software solution.

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt.

The file legal_notices.txt is also located in the installation folder of managed applications.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Adobe, Acrobat, Flash, PostScript, Reader, Shockwave are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

AMD64 is a trademark or registered trademark of Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS and 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, App Store, AppleScript, FileVault, iPadOS, iPhone, iTunes, Mac, Mac OS, macOS, OS X, Safari, and QuickTime 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, IOS, Cisco Jabber 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.

Cloudflare, the Cloudflare logo, and Cloudflare Workers are trademarks and/or registered trademarks of Cloudflare, Inc. in the United States and other jurisdictions.

Corel, and CorelDRAW are trademarks or registered trademarks of Corel Corporation and/or its subsidiaries in Canada, the United States and/or other countries.

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, Dalvik, Firebase, Google Chrome, Google Earth, Google Maps, Google Play, Google Public DNS are trademarks of Google LLC.

HUAWEI, EulerOS, HUAWEI CLOUD are trademarks of Huawei Technologies Co., Ltd.

Intel and Core 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, ActiveX, BitLocker, Excel, Hyper-V, InfoPath, Internet Explorer, Microsoft 365, Microsoft Edge, MS-DOS, MultiPoint, Office 365, OneNote, Outlook, PowerPoint, PowerShell, Segoe, Skype, SQL Server, Tahoma, Visio, Win32, Windows, Windows Azure, Windows Media, Windows Mobile, Windows Phone, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

CVE is a registered trademark of The MITRE Corporation.

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.

NetWare is a registered trademark of Novell Inc. in the United States and other countries.

OpenVPN is a registered trademark of OpenVPN, Inc.

Oracle, Java, JavaScript are registered trademarks of Oracle and/or its affiliates.

Parallels, the Parallels logo, and Coherence are trademarks or registered trademarks of Parallels International GmbH.

Python is a trademark or registered trademark of the Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS, Fedora are trademarks or registered trademarks 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.

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 is a trademark and registered trademark 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.

Rocky Linux is a trademark of The Rocky Enterprise Software Foundation.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.