

kaspersky

Kaspersky Security Center 15 Linux

© 2024 AO Kaspersky Lab

Contents

[Kaspersky Security Center Linux Help](#)

[What's new](#)

[About Kaspersky Security Center Linux](#)

[Hardware and software requirements](#)

[Administration Server requirements](#)

[Web Console requirements](#)

[Network Agent requirements](#)

[Compatible Kaspersky applications and solutions](#)

[Unsupported operating systems and platforms](#)

[Unsupported operating systems and platforms. Administration Server](#)

[Unsupported operating systems and platforms. Kaspersky Security Center Web Console Server](#)

[Unsupported operating systems and platforms. Network Agent](#)

[Distribution kit](#)

[About compatibility of Administration Server and Kaspersky Security Center Web Console](#)

[Comparison of Kaspersky Security Center: Windows-based vs. Linux-based](#)

[About Kaspersky Security Center Cloud Console](#)

[Architecture and basic concepts](#)

[Architecture](#)

[Deployment diagram of Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console](#)

[Ports used by Kaspersky Security Center Linux](#)

[Ports used by Kaspersky Security Center Web Console](#)

[Basic concepts](#)

[Administration Server](#)

[Hierarchy of Administration Servers](#)

[Virtual Administration Server](#)

[Web Server](#)

[Network Agent](#)

[Administration groups](#)

[Managed device](#)

[Unassigned device](#)

[Administrator's workstation](#)

[Management web plug-in](#)

[Policies](#)

[Policy profiles](#)

[Tasks](#)

[Task scope](#)

[How local application settings relate to policies](#)

[Distribution point](#)

[Connection gateway](#)

[Schemas for data traffic and port usage](#)

[Administration Server and managed devices on LAN](#)

[Primary Administration Server on LAN and two secondary Administration Servers](#)

[Administration Server on LAN, managed devices on internet, firewall in use](#)

[Administration Server on LAN, managed devices on internet, connection gateway in use](#)

[Administration Server in DMZ, managed devices on internet](#)

[Interaction of Kaspersky Security Center Linux components and security applications: more information](#)

[Conventions used in interaction schemas](#)

[Administration Server and DBMS](#)

[Administration Server and client device: Managing the security application](#)

[Upgrading software on a client device through a distribution point](#)

[Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server](#)

[Hierarchy of Administration Servers with a secondary Administration Server in DMZ](#)

[Administration Server, a connection gateway in a network segment, and a client device](#)

[Administration Server and two devices in DMZ: a connection gateway and a client device](#)

[Administration Server and Kaspersky Security Center Web Console](#)

[Getting started](#)

[Installation](#)

[Configuring the MariaDB x64 server for working with Kaspersky Security Center Linux](#)

[Configuring the PostgreSQL or Postgres Pro server for working with Kaspersky Security Center Linux](#)

[Scenario: Authenticating PostgreSQL Server](#)

[Scenario: Authenticating MySQL Server](#)

[Installing Kaspersky Security Center Linux](#)

[Installing Kaspersky Security Center Linux in silent mode](#)

[Installing Kaspersky Security Center Linux on Astra Linux in the closed software environment mode](#)

[Installing Kaspersky Security Center Web Console](#)

[Kaspersky Security Center Web Console installation parameters](#)

[Installing Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode](#)

[Installing Kaspersky Security Center Web Console connected to Administration Server installed on Kaspersky Security Center Linux failover cluster nodes](#)

[Deployment of the Kaspersky Security Center Linux failover cluster](#)

[Scenario: Deployment of Kaspersky Security Center Linux failover cluster](#)

[About Kaspersky Security Center Linux failover cluster](#)

[Preparing a file server for a Kaspersky Security Center Linux failover cluster](#)

[Preparing nodes for a Kaspersky Security Center Linux failover cluster](#)

[Installing Kaspersky Security Center Linux on the Kaspersky Security Center Linux failover cluster nodes](#)

[Starting and stopping cluster nodes manually](#)

[Accounts for working with the DBMS](#)

[Configuring the DBMS account for work with MySQL and MariaDB](#)

[Configuring the DBMS account for work with PostgreSQL and Postgres Pro](#)

[Certificates for work with Kaspersky Security Center Linux](#)

[About Kaspersky Security Center certificates](#)

[Requirements for custom certificates used in Kaspersky Security Center Linux](#)

[Reissuing the certificate for Kaspersky Security Center Web Console](#)

[Replacing certificate for Kaspersky Security Center Web Console](#)

[Converting a PFX certificate to the PEM format](#)

[Scenario: Specifying the custom Administration Server certificate](#)

[Replacing the Administration Server certificate by using the klservcert utility](#)

[Connecting Network Agents to Administration Server by using the klmover utility](#)

[Defining a shared folder](#)

[Signing in to Kaspersky Security Center Web Console and signing out](#)

[Changing the language of the Kaspersky Security Center Web Console interface](#)

[Configuring the MySQL x64 server for working with Kaspersky Security Center Linux](#)

[Quick start wizard](#)

[Step 1. Specifying the internet connection settings](#)

- [Step 2. Downloading required updates](#)
- [Step 3. Selecting the assets to secure](#)
- [Step 4. Selecting encryption in solutions](#)
- [Step 5. Configuring installation of plug-ins for managed applications](#)
- [Step 6. Downloading distribution packages and creating installation packages](#)
- [Step 7. Configuring Kaspersky Security Network](#)
- [Step 8. Selecting the application activation method](#)
- [Step 9. Creating a basic network protection configuration](#)
- [Step 10. Configuring email notifications](#)
- [Step 11. Closing the quick start wizard](#)

[Protection deployment wizard](#)

- [Starting Protection deployment wizard](#)
- [Step 1. Selecting the installation package](#)
- [Step 2. Selecting a method for distribution of key file or activation code](#)
- [Step 3. Selecting Network Agent version](#)
- [Step 4. Selecting devices](#)
- [Step 5. Specifying the remote installation task settings](#)
- [Step 6. Removing incompatible applications before installation](#)
- [Step 7. Moving devices to Managed devices](#)
- [Step 8. Selecting accounts to access devices](#)
- [Step 9. Starting installation](#)

[Upgrading Kaspersky Security Center Linux](#)

- [Upgrading Kaspersky Security Center Linux by using the installation file](#)
- [Upgrading Kaspersky Security Center Linux through backup](#)
- [Upgrading Kaspersky Security Center Linux on the Kaspersky Security Center Linux failover cluster nodes](#)
- [Upgrading Kaspersky Security Center Web Console](#)
- [Upgrading Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode](#)

[Migration to Kaspersky Security Center Linux](#)

- [Exporting group objects from Kaspersky Security Center Windows](#)
- [Importing the export file to Kaspersky Security Center Linux](#)
- [Switching managed devices to be under management of Kaspersky Security Center Linux](#)

[Configuring Administration Server](#)

- [Configuring the connection of Kaspersky Security Center Web Console to Administration Server](#)
- [Configuring an allowlist of IP addresses to log in to Kaspersky Security Center Linux](#)
- [Configuring internet access settings for Administration Server](#)
- [Hierarchy of Administration Servers](#)
- [Creating a hierarchy of Administration Servers: adding a secondary Administration Server](#)
- [Viewing the list of secondary Administration Servers](#)
- [Managing virtual Administration Servers](#)
 - [Creating a virtual Administration Server](#)
 - [Enabling and disabling a virtual Administration Server](#)
 - [Assigning an administrator for a virtual Administration Server](#)
 - [Changing the Administration Server for client devices](#)
 - [Deleting a virtual Administration Server](#)
- [Viewing log of connections to the Administration Server](#)
- [Setting the maximum number of events in the event repository](#)
- [Moving Administration Server to another device](#)
- [Changing DBMS credentials](#)

[Backup copying and restoration of Administration Server data](#)

[Creating an Administration Server data backup task](#)

[Using the klbackup utility to back up and recover data](#)

[Administration Server maintenance](#)

[Deleting a hierarchy of Administration Servers](#)

[Access to public DNS servers](#)

[Configuring the interface](#)

[Encrypt communication with TLS](#)

[Discovering networked devices](#)

[Scenario: Discovering networked devices](#)

[IP range polling](#)

[Adding and modifying an IP range](#)

[Zeroconf polling](#)

[Domain controller polling](#)

[Configuring a Samba domain controller](#)

[Using VDI dynamic mode on client devices](#)

[Enabling VDI dynamic mode in the properties of an installation package for Network Agent](#)

[Moving devices from VDI to an administration group](#)

[Deployment best practices](#)

[Hardening Guide](#)

[Administration Server deployment](#)

[Connection safety](#)

[Accounts and authentication](#)

[Managing protection of Administration Server](#)

[Managing protection of client devices](#)

[Configuring protection for managed applications](#)

[Administration Server maintenance](#)

[Event transfer to third-party systems](#)

[Preparation for deployment](#)

[Planning Kaspersky Security Center Linux deployment](#)

[Typical schemes of protection system deployment](#)

[About planning Kaspersky Security Center Linux deployment in an organization's network](#)

[Selecting a structure for protection of an enterprise](#)

[Standard configurations of Kaspersky Security Center Linux](#)

[Standard configuration: Single office](#)

[Standard configuration: A few large-scale offices run by their own administrators](#)

[Standard configuration: Multiple small remote offices](#)

[Selecting a DBMS](#)

[Providing internet access to Administration Server](#)

[Internet access: Administration Server on a local network](#)

[Internet access: Administration Server in DMZ](#)

[Internet access: Network Agent as connection gateway in DMZ](#)

[About distribution points](#)

[Calculating the number and configuration of distribution points](#)

[Virtual Administration Servers](#)

[Network settings for interaction with external services](#)

[Deploying Network Agent and the security application](#)

[Initial deployment](#)

[Configuring installers](#)

[Installation packages](#)

[About remote installation tasks in Kaspersky Security Center Linux](#)

[Deployment by capturing and copying the image of a device](#)

[Network Agent disk cloning mode](#)

[Forced deployment through the remote installation task of Kaspersky Security Center Linux](#)

[Running stand-alone packages created by Kaspersky Security Center Linux](#)

[Remote installation of applications on devices with Network Agent installed](#)

[Managing device restarts in the remote installation task](#)

[Suitability of databases updating in an installation package of a security application](#)

[Monitoring the deployment](#)

[Configuring installers](#)

[General information](#)

[Installation in silent mode \(with a response file\)](#)

[Partial installation configuration through setup.exe](#)

[Administration Server installation parameters](#)

[Network Agent installation parameters](#)

[Virtual infrastructure](#)

[Tips on reducing the load on virtual machines](#)

[Support of dynamic virtual machines](#)

[Support of virtual machines copying](#)

[Support of file system rollback for devices with Network Agent](#)

[Local installation of applications](#)

[Local installation of Network Agent](#)

[Installing Network Agent in silent mode](#)

[Local installation of the application management plug-in](#)

[Installing applications in silent mode](#)

[Installing applications by using stand-alone packages](#)

[Network Agent installation package settings](#)

[Manual setup of the group task for scanning a device with Kaspersky Endpoint Security](#)

[Managing client devices](#)

[Settings of a managed device](#)

[Creating administration groups](#)

[Device moving rules](#)

[Creating device moving rules](#)

[Copying device moving rules](#)

[Conditions for a device moving rule](#)

[Adding devices to an administration group manually](#)

[Moving devices or clusters to an administration group manually](#)

[About clusters and server arrays](#)

[Properties of a cluster or server array](#)

[Adjustment of distribution points and connection gateways](#)

[Standard configuration of distribution points: Single office](#)

[Standard configuration of distribution points: Multiple small remote offices](#)

[Calculating the number and configuration of distribution points](#)

[Assigning distribution points automatically](#)

[Assigning distribution points manually](#)

[Modifying the list of distribution points for an administration group](#)

[Enabling a push server](#)

[About device statuses](#)

[Configuring the switching of device statuses](#)

[Device selections](#)

[Viewing the device list from a device selection](#)

[Creating a device selection](#)

[Configuring a device selection](#)

[Exporting the device list from a device selection](#)

[Removing devices from administration groups in a selection](#)

[Device tags](#)

[About device tags](#)

[Creating a device tag](#)

[Renaming a device tag](#)

[Deleting a device tag](#)

[Viewing devices to which a tag is assigned](#)

[Viewing tags assigned to a device](#)

[Tagging a device manually](#)

[Removing an assigned tag from a device](#)

[Viewing rules for tagging devices automatically](#)

[Editing a rule for tagging devices automatically](#)

[Creating a rule for tagging devices automatically](#)

[Running rules for auto-tagging devices](#)

[Deleting a rule for tagging devices automatically](#)

[Data encryption and protection](#)

[Viewing the list of encrypted drives](#)

[Viewing the list of encryption events](#)

[Creating and viewing encryption reports](#)

[Granting access to an encrypted drive in offline mode](#)

[Changing the Administration Server for client devices](#)

[Viewing and configuring the actions when devices show inactivity](#)

[Sending messages to device users](#)

[Turning on, turning off, and restarting client devices remotely](#)

[Deploying Kaspersky applications](#)

[Scenario: Kaspersky applications deployment](#)

[Adding management plug-ins for Kaspersky applications](#)

[Downloading and creating installation packages for Kaspersky applications](#)

[Creating installation packages from a file](#)

[Creating stand-alone installation packages](#)

[Changing the limit on the size of custom installation package data](#)

[Installing Network Agent for Linux in silent mode \(with an answer file\)](#)

[Preparing a device running Astra Linux in the closed software environment mode for installation of Network Agent](#)

[Viewing the list of stand-alone installation packages](#)

[Distributing installation packages to secondary Administration Servers](#)

[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](#)

[Specifying settings for remote installation on Unix devices](#)

[Replacing third-party security applications](#)

[Removing applications or software updates remotely](#)

[Preparing a device running SUSE Linux Enterprise Server 15 for installation of Network Agent](#)

[Preparing a Windows device for remote installation. Riprep utility](#)

[Preparing a Windows device for remote installation in interactive mode](#)

[Preparing a Windows device for remote installation in silent mode](#)

[Licensing](#)

[About licensing of Kaspersky Security Center Linux](#)

[About the End User License Agreement](#)

[About the license](#)

[About the license certificate](#)

[About the license key](#)

[Viewing the Privacy Policy](#)

[Kaspersky Security Center licensing options](#)

[About the key file](#)

[About data provision](#)

[About the subscription](#)

[Activating Kaspersky Security Center Linux](#)

[Licensing of managed Kaspersky applications](#)

[Licensing of managed applications](#)

[Adding a license key to the Administration Server repository](#)

[Deploying a license key to client devices](#)

[Automatic distribution of a license key](#)

[Viewing information about license keys in use](#)

[Events of the licensing limit exceeded](#)

[Deleting a license key from the repository](#)

[Revoking consent with an End User License Agreement](#)

[Renewing licenses for Kaspersky applications](#)

[Using Kaspersky Marketplace to choose Kaspersky business solutions](#)

[Configuring Kaspersky applications](#)

[Scenario: Configuring network protection](#)

[About device-centric and user-centric security management approaches](#)

[Policy setup and propagation: Device-centric approach](#)

[Policy setup and propagation: User-centric approach](#)

[Policies and policy profiles](#)

[About policies and policy profiles](#)

[About lock and locked settings](#)

[Inheritance of policies and policy profiles](#)

[Hierarchy of policies](#)

[Policy profiles in a hierarchy of policies](#)

[How settings are implemented on a managed device](#)

[Managing policies](#)

[Viewing the list of policies](#)

[Creating a policy](#)

[General policy settings](#)

[Modifying a policy](#)

[Enabling and disabling a policy inheritance option](#)

[Copying a policy](#)

[Moving a policy](#)

[Exporting a policy](#)

[Importing a policy](#)

[Forced synchronization](#)

[Viewing the policy distribution status chart](#)

[Deleting a policy](#)

[Managing policy profiles](#)

[Viewing the profiles of a policy](#)

[Changing a policy profile priority](#)

[Creating a policy profile](#)

[Copying a policy profile](#)

[Creating a policy profile activation rule](#)

[Deleting a policy profile](#)

[Network Agent policy settings](#)

[Usage of Network Agent for Windows, Linux, and macOS: comparison](#)

[Comparison of Network Agent settings by operating systems](#)

[Manual setup of the Kaspersky Endpoint Security policy](#)

[Configuring Kaspersky Security Network](#)

[Checking the list of the networks protected by Firewall](#)

[Disabling the scan of network devices](#)

[Excluding software details from the Administration Server memory](#)

[Configuring access to the Kaspersky Endpoint Security for Windows interface on workstations](#)

[Saving important policy events in the Administration Server database](#)

[Manual setup of the group update task for Kaspersky Endpoint Security](#)

[Kaspersky Security Network \(KSN\)](#)

[About KSN](#)

[Setting up access to 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](#)

[Managing tasks](#)

[About tasks](#)

[About task scope](#)

[Creating a task](#)

[Starting a task manually](#)

[Viewing the task list](#)

[General task settings](#)

[Exporting a task](#)

[Importing a task](#)

[Starting the Change tasks password wizard](#)

[Step 1. Specifying credentials](#)

[Step 2. Selecting an action to take](#)

[Step 3. Viewing the results](#)

[Viewing task run results stored on the Administration Server](#)

[Application tags](#)

[About 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](#)

[Granting offline access to the external device blocked by Device Control](#)

[Using the klscflag utility to open port 13291](#)

[Registering Kaspersky Industrial CyberSecurity for Networks application in Kaspersky Security Center Web Console](#)

[Managing users and user roles](#)

[About user accounts](#)

[About user roles](#)

[Configuring access rights to application features. Role-based access control](#)

[Access rights to application features](#)

[Predefined user roles](#)

[Assigning access rights to specific objects](#)

[Assigning access rights to users and groups](#)

[Adding an account of an internal user](#)

[Creating a security group](#)

[Editing an account of an internal user](#)

[Editing a security group](#)

[Assigning a role to a user or a security group](#)

[Adding user accounts to an internal security group](#)

[Assigning a user as a device owner](#)

[Enabling account protection from unauthorized modification](#)

[Two-step verification](#)

[Scenario: configuring two-step verification for all users](#)

[About two-step verification for an account](#)

[Enabling two-step verification for your own account](#)

[Enabling two-step verification for all users](#)

[Disabling two-step verification for a user account](#)

[Disabling two-step verification for all users](#)

[Excluding accounts from two-step verification](#)

[Configuring two-step verification for your own account](#)

[Prohibit new users from setting up two-step verification for themselves](#)

[Generating a new secret key](#)

[Editing the name of a security code issuer](#)

[Changing the number of allowed password entry attempts](#)

[Deleting 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](#)

[API Reference Guide](#)

[Updating Kaspersky databases and applications](#)

[Scenario: Regular updating Kaspersky databases and applications](#)

[About updating Kaspersky databases, software modules, and applications](#)

[Creating the Download updates to the Administration Server repository task](#)

[Verifying downloaded updates](#)

[Creating the task for downloading updates to the repositories of distribution points](#)

[Adding sources of updates for the Download updates to the Administration Server repository task](#)

[About using diff files for updating Kaspersky databases and software modules](#)

[Enabling the Downloading diff files feature: scenario](#)

[Downloading updates by distribution points](#)

[Updating Kaspersky databases and software modules on offline devices](#)

[Backing up and restoring web plug-ins](#)

[Monitoring, reporting, and audit](#)

[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](#)

[Reports](#)

[Using reports](#)

[Creating a 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 Security Center Linux](#)

[Events of Kaspersky Security Center Linux components](#)

[Data structure of event type description](#)

[Administration Server events](#)

[Administration Server critical events](#)

[Administration Server functional failure events](#)

[Administration Server warning events](#)

[Administration Server informational events](#)

[Network Agent events](#)

[Network Agent 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 details of an event](#)

[Exporting events to a file](#)

[Viewing an object history from an event](#)

- [Deleting events](#)
- [Deleting event selections](#)
- [Setting the storage term for an event](#)
- [Blocking frequent events](#)
 - [About blocking frequent events](#)
 - [Managing frequent events blocking](#)
 - [Removing blocking of frequent events](#)
- [Event processing and storage on the Administration Server](#)
- [Notifications and device statuses](#)
 - [Using notifications](#)
 - [Viewing onscreen notifications](#)
 - [About device statuses](#)
 - [Configuring the switching of device statuses](#)
 - [Configuring notification delivery](#)
 - [Testing notifications](#)
 - [Event notifications displayed by running an executable file](#)
- [Kaspersky announcements](#)
 - [About Kaspersky announcements](#)
 - [Specifying Kaspersky announcements settings](#)
 - [Disabling Kaspersky announcements](#)
- [Exporting events to SIEM systems](#)
 - [Scenario: configuring event export to SIEM systems](#)
 - [Before you begin](#)
 - [About event export](#)
 - [About configuring event export in a SIEM system](#)
 - [Marking of events for export to SIEM systems in Syslog format](#)
 - [About marking events for export to SIEM system in the Syslog format](#)
 - [Marking events of a Kaspersky application for export in the Syslog format](#)
 - [Marking general events for export in Syslog format](#)
 - [About exporting events using Syslog format](#)
 - [Configuring Kaspersky Security Center Linux for export of events to a SIEM system](#)
 - [Exporting events directly from the database](#)
 - [Creating an SQL query using the klsqI2 utility](#)
 - [Example of an SQL query in the klsqI2 utility](#)
 - [Viewing the Kaspersky Security Center Linux database name](#)
 - [Viewing export results](#)
- [Managing object revisions](#)
 - [About object revisions](#)
 - [Rolling back an object to a previous revision](#)
- [Deletion of objects](#)
- [Downloading and deleting files from Quarantine and Backup](#)
 - [Downloading files from Quarantine and Backup](#)
 - [About removing objects from the Quarantine, Backup, or Active threats 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 Kaspersky Security Center Linux Network Agent 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](#)

[Managing third-party applications on client devices](#)

[Scenario: Application Management](#)

[About Application Control](#)

[Obtaining and viewing a list of applications installed on client devices](#)

[Obtaining and viewing a list of executable files stored on client devices](#)

[Creating an application category with content added manually](#)

[Creating an application category that includes executable files from selected devices](#)

[Creating an application category that includes executable files from selected folder](#)

[Viewing the list of application categories](#)

[Configuring Application Control in the Kaspersky Endpoint Security for Windows policy](#)

[Adding event-related executable files to the application category](#)

[Sizing Guide](#)

[About this Guide](#)

[Calculations for Administration Servers](#)

[Calculation of hardware resources for the Administration Server](#)

[Hardware requirements for the DBMS and the Administration Server](#)

[Calculation of database space](#)

[Calculation of disk space](#)

[Calculation of the number and configuration of Administration Servers](#)

[Recommendations for connecting dynamic virtual machines to Kaspersky Security Center](#)

[Calculations for distribution points and connection gateways](#)

[Requirements for a distribution point](#)

[Calculating the number and configuration of distribution points](#)

[Calculation of the number of connection gateways](#)

[Logging of information about events for tasks and policies](#)

[Specific considerations and optimal settings of certain tasks](#)

[Device discovery frequency](#)

[Administration Server data backup task and database maintenance task](#)

[Group tasks for updating Kaspersky Endpoint Security](#)

[Software inventory task](#)

[Details of network load spread among Administration Server and protected devices](#)

[Traffic consumption under various scenarios](#)

[Average traffic usage per 24 hours](#)

[Contact Technical Support](#)

[How to get technical support](#)

[Technical support via Kaspersky CompanyAccount](#)

[Sources of information about the application](#)

[Known issues](#)

[Glossary](#)

[Active key](#)

[Additional subscription key](#)
[Administration Console](#)
[Administration group](#)
[Administration Server](#)
[Administration Server certificate](#)
[Administration Server client \(Client device\)](#)
[Administration Server data backup](#)
[Administrator rights](#)
[Administrator's workstation](#)
[Anti-virus databases](#)
[Anti-virus protection service provider](#)
[Application Shop](#)
[Authentication Agent](#)
[Available update](#)
[Backup folder](#)
[Broadcast domain](#)
[Centralized application management](#)
[Client administrator](#)
[Configuration profile](#)
[Connection gateway](#)
[Demilitarized zone \(DMZ\)](#)
[Device owner](#)
[Direct application management](#)
[Distribution point](#)
[Event repository](#)
[Event severity](#)
[Group task](#)
[Home Administration Server](#)
[HTTPS](#)
[Incompatible application](#)
[Installation package](#)
[Internal users](#)
[JavaScript](#)
[Kaspersky Private Security Network \(KPSN\)](#)
[Kaspersky Security Center Linux Administrator](#)
[Kaspersky Security Center Linux Web Server](#)
[Kaspersky Security Center Operator](#)
[Kaspersky Security Center System Health Validator \(SHV\)](#)
[Kaspersky update servers](#)
[Key file](#)
[License term](#)
[Licensed applications group](#)
[Local installation](#)
[Local task](#)
[Managed devices](#)
[Manual installation](#)
[Network Agent](#)
[Network anti-virus protection](#)

[Network protection status](#)
[Policy](#)
[Profile](#)
[Program settings](#)
[Protection status](#)
[Provisioning profile](#)
[Remote installation](#)
[Restoration](#)
[Restoration of Administration Server data](#)
[Role group](#)
[Service provider's administrator](#)
[Shared certificate](#)
[SSL](#)
[Task](#)
[Task for specific devices](#)
[Task settings](#)
[Update](#)
[Virtual Administration Server](#)
[Information about third-party code](#)
[Trademark notices](#)

New functions

- [What's new](#)

Hardware and software requirements

- [Administration Server requirements](#)
- [Web Console requirements](#)
- [Network Agent requirements](#)

Getting started

- [Installation](#)
- [Quick start wizard](#)
- [Protection deployment wizard](#)

Licensing and activation

- [Activating Kaspersky Security Center Linux](#)
- [Licensing of managed applications](#)

Deployment and configuration

- [Discovering networked devices](#)
- [Adjustment of distribution points and/or connection gateways](#)
- [Replacing third-party security applications](#)
- [Kaspersky applications. Centralized deployment](#)
- [Configuring network protection](#)

- [Kaspersky applications. Updating databases and software modules](#)

Monitoring

- [Monitoring and reporting](#)

Additional features

- [Exporting events to SIEM systems](#)
- [Sizing Guide](#) (Online Help only)

What's new

Kaspersky Security Center 15 Linux

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

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

- Kaspersky Security Center Linux now supports cluster technology. If an administration group contains [clusters or server arrays](#), the **Managed devices** page displays two tabs—one for individual devices, and one for clusters and server arrays. After the managed devices are detected as cluster nodes, the cluster is added as an individual object to the **Clusters and server arrays** tab. The cluster nodes are listed on the **Devices** tab, along with other managed devices.
- [Support for some platforms by Kaspersky Security Center Linux](#) is ended because these platforms are no longer supported by their vendors.

Kaspersky Security Center 14.2 Linux

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

- In an [Administration Server hierarchy](#), a Linux-based Administration Server can now act as a primary Server and can manage Linux-based or Windows-based Servers acting as a secondary one.
- Kaspersky Security Center Linux now supports [Kaspersky Security Network \(KSN\)](#), [KSN Proxy service](#), and Kaspersky Private Security Network (KPSN).
- [Kaspersky Security Center Linux now supports Kaspersky Endpoint Security for Windows](#) as a managed application.
Remote installation of Network Agent for Windows on client devices is possible only by using operating system tools through Windows-based distribution points.
- [Data on Windows-based managed devices can now be encrypted](#) to reduce the risk of unintentional leakage of sensitive and corporate data if a laptop or hard drive is stolen or lost. This feature is implemented through Kaspersky Endpoint Security for Windows.
- Kaspersky Security Center Linux allows you to download and update both [distribution packages of Kaspersky applications](#) and management web plug-ins right in the user interface of Kaspersky Security Center Linux.
- By default, information about applications installed on the Linux-based and Windows-based managed devices is sent to Administration Server.
- Access to Kaspersky servers is now verified automatically. If access to the servers by using the system DNS is not possible, the application uses the public DNS.
- Sensitive data that is transferred between the primary Administration Server, secondary Administration Servers, and Network Agents is now protected with the AES encryption algorithm.
- [User rights on a virtual Administration Server](#) are available for configuration any time, independently from the primary Administration Server. Also, you can assign primary Server users the rights to manage a virtual Server.
- Kaspersky Security Center Linux now supports work with the following [DBMSs](#):
 - PostgreSQL 13.x
 - PostgreSQL 14.x
 - Postgres Pro 13.x (all editions)
 - Postgres Pro 14.x (all editions)
- You can use Kaspersky Security Center Web Console to [export policies](#) and [tasks](#) to a file, and then [import the policies](#) and [tasks](#) to Kaspersky Security Center Windows or Kaspersky Security Center Linux.

- The **Do not use proxy server** option has been removed from the following tasks:
 - *Download updates to the Administration Server repository*
 - *Download updates to the repositories of distribution points*

Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux has several new features and improvements:

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

About Kaspersky Security Center Linux

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

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

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

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

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

Using Kaspersky Security Center, you can do the following:

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

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

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

Hardware and software requirements

- [Administration Server requirements](#)
- [Web Console requirements](#)
- [Network Agent requirements](#)

Administration Server requirements

Minimum hardware requirements:

- CPU with operating frequency of 1,4 GHz or higher.
- RAM: 4 GB.
- Available disk space: 10 GB (/var/opt/kaspersky/klnagent_srv).

The following operating systems are supported:

- Debian GNU/Linux 10.x (Buster) 64-bit
- Debian GNU/Linux 11.x (Bullseye) 64-bit
- Debian GNU/Linux 12 (Bookworm) 64-bit
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64-bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-bit
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bit
- CentOS 7.x 64-bit
- CentOS Stream 9 64-bit
- Red Hat Enterprise Linux Server 7.x 64-bit
- Red Hat Enterprise Linux Server 8.x 64-bit
- Red Hat Enterprise Linux Server 9.x 64-bit
- SUSE Linux Enterprise Server 12 (all Service Packs) 64-bit
- SUSE Linux Enterprise Server 15 (all Service Packs) 64-bit
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6) 64-bit
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7) 64-bit

- Astra Linux Common Edition (operational update 2.12) 64-bit
- ALT SP Server 10 64-bit
- ALT Server 10 64-bit
- ALT Server 9.2 64-bit
- ALT 8 SP Server (LKNV.11100-01) 64-bit
- ALT 8 SP Server (LKNV.11100-02) 64-bit
- ALT 8 SP Server (LKNV.11100-03) 64-bit
- Oracle Linux 7 64-bit
- Oracle Linux 8 64-bit
- Oracle Linux 9 64-bit
- RED OS 7.3 Server 64-bit
- RED OS 7.3 Certified Edition 64-bit
- ROSA COBALT 7.9 64-bit

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

The following virtualization platforms are supported:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64-bit
- Microsoft Hyper-V Server 2012 R2 64-bit
- Microsoft Hyper-V Server 2016 64-bit
- Microsoft Hyper-V Server 2019 64-bit
- Microsoft Hyper-V Server 2022 64-bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x

- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- Kernel-based Virtual Machine (all Linux operating systems supported by Administration server)

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

- MySQL 5.7 Community 32-bit/64-bit
- MySQL 8.0 32-bit/64-bit
- MariaDB 10.1 (build 10.1.30 and later) 32-bit/64-bit
- MariaDB 10.3 (build 10.3.22 and later) 32-bit/64-bit
- MariaDB 10.4 (build 10.4.26 and later) 32-bit/64-bit
- MariaDB 10.5 (build 10.5.17 and later) 32-bit/64-bit
- MariaDB Galera Cluster 10.3 32-bit/64-bit with InnoDB storage engine
- PostgreSQL 13.x 64-bit
- PostgreSQL 14.x 64-bit
- PostgreSQL 15.x 64-bit
- Postgres Pro 13.x 64-bit (all editions)
- Postgres Pro 14.x 64-bit (all editions)
- Postgres Pro 15.x 64-bit (all editions)
- Platform V Pangolin 5.4.0 64-bit
- Jatoba 4 64-bit

Web Console requirements

Kaspersky Security Center Web Console Server

Minimum hardware requirements:

- CPU: 4 cores, operating frequency of 2.5 GHz.
- RAM: 8 GB.
- Available disk space: 40 GB (/var/opt/kaspersky).

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

- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 12 (Bookworm)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- CentOS Stream 9
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- SUSE Linux Enterprise Server 12 (all Service Packs)
- SUSE Linux Enterprise Server 15 (all Service Packs)
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6)
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7)
- Astra Linux Common Edition (operational update 2.12)
- ALT SP Server 10
- ALT Server 10
- ALT Server 9.2
- ALT 8 SP Server (LKNV.11100-01)
- ALT 8 SP Server (LKNV.11100-02)
- ALT 8 SP Server (LKNV.11100-03)
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- ROSA COBALT 7.9

- Kernel-based Virtual Machine (all Linux operating systems supported by Kaspersky Security Center Web Console Server)

Client devices

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

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

Browsers:

- Google Chrome 100.0.4896.88 or later (official build)
- Microsoft Edge 100 or later
- Safari 15 on macOS
- "Yandex" Browser 23.5.0.2271 or later
- Mozilla Firefox Extended Support Release 102.0 or later

Network Agent requirements

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.
- Available disk space: 1 GB.

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

The following operating systems are supported:

- 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 LTSC 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2016 LTSC 32-bit/64-bit
- Microsoft Windows 10 IoT Enterprise 2015 LTSC 32-bit/64-bit
- Microsoft Windows 10 IoT Enterprise 2016 LTSC 32-bit/64-bit

- Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit
- Microsoft Windows 10 IoT Enterprise version 1703 32-bit/64-bit
- Microsoft Windows 10 IoT Enterprise version 1709 32-bit/64-bit
- Microsoft Windows 10 IoT Enterprise version 1803 32-bit/64-bit
- Microsoft Windows 10 IoT Enterprise version 1809 32-bit/64-bit
- Microsoft Windows 10 20H2 IoT Enterprise 32-bit/64-bit
- Microsoft Windows 10 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 Home RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Home RS5 (October 2018) 32-bit/64-bit
- Microsoft Windows 10 Pro RS5 (October 2018) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS5 (October 2018) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS5 (October 2018) 32-bit/64-bit
- Microsoft Windows 10 Education RS5 (October 2018) 32-bit/64-bit
- Microsoft Windows 10 Home 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro 19H1 32-bit/64-bit

- Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit
- Microsoft Windows 10 Education 19H1 32-bit/64-bit
- Microsoft Windows 10 Home 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit
- Microsoft Windows 10 Education 19H2 32-bit/64-bit
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-bit/64-bit
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-bit/64-bit
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-bit/64-bit
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-bit/64-bit
- Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-bit/64-bit
- Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-bit/64-bit
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-bit/64-bit
- Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-bit/64-bit
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-bit/64-bit
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-bit/64-bit
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-bit/64-bit
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-bit/64-bit
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-bit/64-bit
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-bit/64-bit
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-bit/64-bit
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-bit/64-bit
- Microsoft Windows 10 Home 22H2 (October 2023 Update) 32-bit/64-bit
- Microsoft Windows 10 Pro 22H2 (October 2023 Update) 32-bit/64-bit
- Microsoft Windows 10 Enterprise 22H2 (October 2023 Update) 32-bit/64-bit
- Microsoft Windows 10 Education 22H2 (October 2023 Update) 32-bit/64-bit

- Microsoft Windows 11 Home 64-bit
- Microsoft Windows 11 Pro 64-bit
- Microsoft Windows 11 Enterprise 64-bit
- Microsoft Windows 11 Education 64-bit
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 Pro 32-bit/64-bit
- Microsoft Windows 8.1 Enterprise 32-bit/64-bit
- Microsoft Windows 8 Pro 32-bit/64-bit
- Microsoft Windows 8 Enterprise 32-bit/64-bit
- Microsoft Windows 7 Professional with Service Pack 1 and later 32-bit/64-bit
- Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and later 32-bit/64-bit
- Microsoft Windows 7 Home Basic/Premium with Service Pack 1 and later 32-bit/64-bit
- Microsoft Windows XP Professional with Service Pack 2 32-bit/64-bit (supported by Network Agent version 10.5.1781 only)
- Microsoft Windows XP Professional with Service Pack 3 and later 32-bit (supported by Network Agent version 14.0.0.20023)
- Microsoft Windows XP Professional for Embedded Systems with Service Pack 3 32-bit (supported by Network Agent version 14.0.0.20023)
- Windows MultiPoint Server 2011 Standard/Premium 64-bit
- Windows Server 2008 Foundation with Service Pack 2 32-bit/64-bit
- Windows Server 2008 with Service Pack 2 (all editions) 32-bit/64-bit
- Windows Server 2008 R2 Datacenter with Service Pack 1 and later 64-bit
- Windows Server 2008 R2 Enterprise with Service Pack 1 and later 64-bit
- Windows Server 2008 R2 Foundation with Service Pack 1 and later 64-bit
- Windows Server 2008 R2 Core Mode with Service Pack 1 and later 64-bit
- Windows Server 2008 R2 Standard with Service Pack 1 and later 64-bit
- Windows Server 2008 R2 with Service Pack 1 (all editions) 64-bit
- Windows Server 2012 Server Core 64-bit
- Windows Server 2012 Datacenter 64-bit
- Windows Server 2012 Essentials 64-bit

- Windows Server 2012 Foundation 64-bit
- Windows Server 2012 Standard 64-bit
- Windows Server 2012 R2 Server Core 64-bit
- Windows Server 2012 R2 Datacenter 64-bit
- Windows Server 2012 R2 Essentials 64-bit
- Windows Server 2012 R2 Foundation 64-bit
- Windows Server 2012 R2 Standard 64-bit
- Windows Server 2016 Datacenter (LTSC) 64-bit
- Windows Server 2016 Standard (LTSC) 64-bit
- Windows Server 2016 Server Core (Installation Option) (LTSC) 64-bit
- Windows Server 2019 Standard 64-bit
- Windows Server 2019 Datacenter 64-bit
- Windows Server 2019 Core 64-bit
- Windows Server 2022 Standard 64-bit
- Windows Server 2022 Datacenter 64-bit
- Windows Server 2022 Core 64-bit
- Debian GNU/Linux 10.x (Buster) 32-bit/64-bit
- Debian GNU/Linux 11.x (Bullseye) 32-bit/64-bit
- Debian GNU/Linux 12 (Bookworm) 32-bit/64-bit
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32-bit/64-bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-bit/64-bit
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bit
- CentOS 7.x 64-bit
- CentOS Stream 9 64-bit
- Red Hat Enterprise Linux Server 6.x 32-bit/64-bit
- Red Hat Enterprise Linux Server 7.x 64-bit
- Red Hat Enterprise Linux Server 8.x 64-bit
- Red Hat Enterprise Linux Server 9.x 64-bit

- SUSE Linux Enterprise Server 12 (all Service Packs) 64-bit
- SUSE Linux Enterprise Server 15 (all Service Packs) 64-bit
- SUSE Linux Enterprise Desktop 15 with Service Pack 3 ARM 64-bit
- openSUSE 15 64-bit
- EulerOS 2.0 SP8 ARM
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6) 64-bit
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7) 64-bit
- Astra Linux Common Edition (operational update 2.12) 64-bit
- Astra Linux Special Edition RUSB.10152-02 (operational update 4.7) ARM 64-bit
- ALT SP Server 10 64-bit
- ALT SP Workstation 10 64-bit
- ALT Server 10 64-bit
- ALT Server 9.2 64-bit
- ALT Workstation 9.2 32-bit/64-bit
- ALT Workstation 10 32-bit/64-bit
- ALT 8 SP Server (LKNV.11100-01) 64-bit
- ALT 8 SP Server (LKNV.11100-02) 64-bit
- ALT 8 SP Server (LKNV.11100-03) 64-bit
- ALT 8 SP Workstation (LKNV.11100-01) 32-bit/64-bit
- ALT 8 SP Workstation (LKNV.11100-02) 32-bit/64-bit
- ALT 8 SP Workstation (LKNV.11100-03) 32-bit/64-bit
- Mageia 4 32-bit
- Oracle Linux 7 64-bit
- Oracle Linux 8 64-bit
- Oracle Linux 9 64-bit
- Linux Mint 20.x 64-bit
- AlterOS 7.5 and later 64-bit
- GosLinux IC6 64-bit

- RED OS 7.3 Server 64-bit
- RED OS 7.3 Certified Edition 64-bit
- ROSA COBALT 7.9 64-bit
- ROSA CHROME 12 64-bit
- macOS Big Sur (11.x)
- macOS Monterey (12.x)
- macOS Ventura (13.x)
- macOS Sonoma (14.x)

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

The following virtualization platforms are supported:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64-bit
- Microsoft Hyper-V Server 2012 R2 64-bit
- Microsoft Hyper-V Server 2016 64-bit
- Microsoft Hyper-V Server 2019 64-bit
- Microsoft Hyper-V Server 2022 64-bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- Kernel-based Virtual Machine (all Linux operating systems supported by Network Agent)

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

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

In Microsoft Windows XP, [Network Agent might not perform some operations correctly](#).

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

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

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

Compatible Kaspersky applications and solutions

Kaspersky Security Center Linux supports centralized deployment and management of the following Kaspersky applications:

- Kaspersky Endpoint Security for Windows 12.0 or later (supports file servers)
- Kaspersky Endpoint Security for Linux 11.2 or later (supports file servers)
- Kaspersky Endpoint Security for Linux Elbrus Edition 10 or later
- Kaspersky Endpoint Security for Linux ARM Edition 11.2 or later
- Kaspersky Endpoint Security for Mac 11.3 or later
- Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 or later
- Kaspersky Industrial CyberSecurity for Nodes 3.2 or later
- Kaspersky Industrial CyberSecurity for Networks 3.2 or later
- Kaspersky Endpoint Agent 3.15 or later
- Kaspersky Embedded Systems Security for Windows 3.2 or later
- Kaspersky Embedded Systems Security for Linux 3.3 or later

- Kaspersky Security for Virtualization Light Agent 5.2 or later

Refer to the [Product Support Lifecycle webpage](#) for the versions of the applications.

Known issues

Kaspersky Security Center Linux supports management of Kaspersky Endpoint Security for Windows with the following limitations:

- The Adaptive Anomaly Control component is not supported. Kaspersky Security Center Linux does not support Adaptive Anomaly Control rules.
- Kaspersky Sandbox components are not supported.
- The Seamless updates functionality is not available.

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

Unsupported operating systems and platforms

- [Unsupported operating systems and platforms. Administration Server](#)
- [Unsupported operating systems and platforms. Kaspersky Security Center Web Console Server](#)
- [Unsupported operating systems and platforms. Network Agent](#)

Unsupported operating systems and platforms. Administration Server

Administration Server is not compatible with the following operating systems:

- Debian GNU/Linux 7.x (up to 7.8) 32-bit/64-bit
- Debian GNU/Linux 8.x (Jessie) 32-bit/64-bit
- Debian GNU/Linux 9.x (Stretch) 32-bit/64-bit
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32-bit/64-bit
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32-bit/64-bit
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32-bit
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64-bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-bit
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-bit/64-bit
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-bit/64-bit

- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bit/64-bit
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bit/64-bit
- CentOS 6.x (up to 6.6) 64-bit
- CentOS 7.x ARM 64-bit
- CentOS 8.x 64-bit
- Red Hat Enterprise Linux Server 6.x 32-bit/64-bit
- SUSE Linux Enterprise Desktop 12 (all Service Packs) 64-bit
- SUSE Linux Enterprise Desktop 15 (all Service Packs) 64-bit
- SUSE Linux Enterprise Desktop 15 with Service Pack 3 ARM 64-bit
- openSUSE 15 64-bit
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64-bit
- Astra Linux Special Edition 1.5 64-bit
- Astra Linux Special Edition RUSB.10152-02 (operational update 4.7) ARM 64-bit
- ALT Workstation 9.2 32-bit/64-bit
- ALT Workstation 10 32-bit/64-bit
- ALT 8 SP Workstation (LKNV.11100-01) 32-bit/64-bit
- ALT 8 SP Workstation (LKNV.11100-02) 32-bit/64-bit
- ALT 8 SP Workstation (LKNV.11100-03) 32-bit/64-bit
- Mageia 4 32-bit
- Linux Mint 19.x 32-bit
- Linux Mint 20.x 64-bit
- AlterOS 7.5 and later 64-bit
- RED OS 7.3 64-bit
- GosLinux IC6 64-bit
- ROSA Enterprise Linux Server 7.3 64-bit
- ROSA Enterprise Linux Desktop 7.3 64-bit
- ROSA COBALT Workstation 7.3 64-bit

- ROSA COBALT Server 7.3 64-bit
- ROSA CHROME 12 64-bit
- Lotos (Linux core version 4.19.50, DE: MATE) 64-bit

Database server:

- PostgreSQL Pangolin 64-bit
- Microsoft SQL Server 2005 Express 32-bit
- Microsoft SQL Server 2005 (all editions) 32-bit/64-bit
- Microsoft SQL Server 2008 Express 32-bit
- Microsoft SQL Server 2008 (all editions) 32-bit/64-bit
- Microsoft SQL Server 2008 R2 (all editions) 64-bit
- Microsoft SQL Server 2008 R2 with Service Pack 2 (all editions) 64-bit
- Microsoft SQL Server 2012 (all editions) 64-bit
- MySQL 5.0 32-bit/64-bit
- MySQL Enterprise 5.0 32-bit/64-bit
- MySQL Standard Edition 5.5 32-bit/64-bit
- MySQL Enterprise Edition 5.5 32-bit/64-bit
- MySQL Standard Edition 5.6 32-bit/64-bit
- MySQL Enterprise Edition 5.6 32-bit/64-bit
- MySQL Standard Edition 5.7 32-bit/64-bit
- MySQL Enterprise Edition 5.7 32-bit/64-bit
- MySQL 5.6 Community 32-bit/64-bit
- MariaDB Galera Cluster 10.4 32-bit/64-bit

The following virtualization platforms are not supported:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6

- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64-bit
- Microsoft Hyper-V Server 2008 R2 64-bit
- Microsoft Hyper-V Server 2008 R2 with Service Pack 1 and later 64-bit
- Microsoft Virtual PC 2007 (6.0.156.0) 32-bit/64-bit
- Citrix XenServer 5.6
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7
- Parallels Desktop 7
- Parallels Desktop 11
- Parallels Desktop 14
- Parallels Desktop 16
- Oracle VM VirtualBox 4.0.4-70112
- Oracle VM VirtualBox 5.x

Unsupported operating systems and platforms. Kaspersky Security Center Web Console Server

Kaspersky Security Center Web Console Server is not compatible with the following operating systems:

- Debian GNU/Linux 7.x (up to 7.8) 32-bit/64-bit

- Debian GNU/Linux 8.x (Jessie) 32-bit/64-bit
- Debian GNU/Linux 9.x (Stretch) 32-bit/64-bit
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32-bit/64-bit
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32-bit/64-bit
- Ubuntu Server 20.04 LTS (Focal Fossa) ARM 64-bit
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-bit/64-bit
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-bit/64-bit
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bit/64-bit
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bit/64-bit
- CentOS 6.x (up to 6.6) 64-bit
- CentOS 7.x ARM 64-bit
- CentOS 7.x 64-bit
- CentOS 8.x 64-bit
- Red Hat Enterprise Linux Server 6.x 32-bit/64-bit
- SUSE Linux Enterprise Desktop 12 (all Service Packs) 64-bit
- SUSE Linux Enterprise Desktop 15 (all Service Packs) 64-bit
- SUSE Linux Enterprise Desktop 15 with Service Pack 3 ARM 64-bit
- openSUSE 15 64-bit
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64-bit
- Astra Linux Special Edition 1.5 64-bit
- Astra Linux Special Edition RUSB.10152-02 (operational update 4.7) ARM 64-bit
- ALT Workstation 9.2 32-bit/64-bit
- ALT Workstation 10 32-bit/64-bit
- ALT 8 SP Workstation (LKNV.11100-01) 32-bit/64-bit
- ALT 8 SP Workstation (LKNV.11100-02) 32-bit/64-bit
- ALT 8 SP Workstation (LKNV.11100-03) 32-bit/64-bit
- Mageia 4 32-bit

- Linux Mint 19.x 32-bit
- Linux Mint 20.x 64-bit
- AlterOS 7.5 and later 64-bit
- RED OS 7.3 64-bit
- GosLinux IC6 64-bit
- ROSA Enterprise Linux Server 7.3 64-bit
- ROSA Enterprise Linux Desktop 7.3 64-bit
- ROSA COBALT Workstation 7.3 64-bit
- ROSA COBALT Server 7.3 64-bit
- ROSA CHROME 12 64-bit
- Lotos (Linux core version 4.19.50, DE: MATE) 64-bit

Unsupported operating systems and platforms. Network Agent

The following operating systems are not supported:

- Microsoft Windows Embedded POSReady 7 32-bit/64-bit
- Microsoft Windows Embedded 8 Standard 32-bit/64-bit
- Microsoft Windows Embedded 8 Industry Pro 32-bit/64-bit
- Microsoft Windows Embedded 8 Industry Enterprise 32-bit/64-bit
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-bit/64-bit
- Microsoft Windows Embedded 8.1 Industry Update 32-bit/64-bit
- Microsoft Windows 10 Home (Threshold 1, 1507) 32-bit/64-bit
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32-bit/64-bit
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-bit/64-bit
- Microsoft Windows 10 Education (Threshold 1, 1507) 32-bit/64-bit
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-bit
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-bit
- Microsoft Windows 10 Home Threshold 2 (November 2015 Update, 1511) 32-bit/64-bit
- Microsoft Windows 10 Pro Threshold 2 (November 2015 Update, 1511) 32-bit/64-bit

- Microsoft Windows 10 Enterprise Threshold 2 (November 2015 Update, 1511) 32-bit/64-bit
- Microsoft Windows 10 Education Threshold 2 (November 2015 Update, 1511) 32-bit/64-bit
- Microsoft Windows 10 Mobile Threshold 2 (November 2015 Update, 1511) 32-bit
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (November 2015 Update, 1511) 32-bit
- Microsoft Windows 10 Home RS1 (Anniversary Update, 1607) 32-bit/64-bit
- Microsoft Windows 10 Pro RS1 (Anniversary Update, 1607) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS1 (Anniversary Update, 1607) 32-bit/64-bit
- Microsoft Windows 10 Education RS1 (Anniversary Update, 1607) 32-bit/64-bit
- Microsoft Windows 10 Mobile RS1 (Anniversary Update, 1607) 32-bit
- Microsoft Windows 10 Mobile Enterprise RS1 (Anniversary Update, 1607) 32-bit
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-bit/64-bit
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-bit/64-bit
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-bit/64-bit
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-bit
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-bit
- Microsoft Windows 10 Mobile RS3 32-bit
- Microsoft Windows 10 Mobile Enterprise RS3 32-bit
- Microsoft Windows 10 Mobile RS4 32-bit
- Microsoft Windows 10 Mobile Enterprise RS4 32-bit
- Microsoft Windows 10 Mobile RS5 32-bit
- Microsoft Windows 10 Mobile Enterprise RS5 32-bit
- Microsoft Windows 8 (Core) 32-bit/64-bit
- Microsoft Windows 7 Professional 32-bit/64-bit
- Microsoft Windows 7 Enterprise/Ultimate 32-bit/64-bit
- Microsoft Windows 7 Home Basic/Premium 32-bit/64-bit
- Microsoft Windows Vista Business with Service Pack 1 32-bit/64-bit
- Microsoft Windows Vista Enterprise with Service Pack 1 32-bit/64-bit

- Microsoft Windows Vista Ultimate with Service Pack 1 32-bit/64-bit
- Microsoft Windows Vista Business with Service Pack 2 and later 32-bit/64-bit
- Microsoft Windows Vista Enterprise with Service Pack 2 and later 32-bit/64-bit
- Microsoft Windows Vista Ultimate with Service Pack 2 and later 32-bit/64-bit
- Microsoft Windows XP Professional with Service Pack 2 32-bit/64-bit
- Microsoft Windows XP Home with Service Pack 3 and later 32-bit
- Windows Essential Business Server 2008 Standard 64-bit
- Windows Essential Business Server 2008 Premium 64-bit
- Windows Small Business Server 2003 Standard with Service Pack 1 32-bit
- Windows Small Business Server 2003 Premium with Service Pack 1 32-bit
- Windows Small Business Server 2003 R2 Standard 32-bit
- Windows Small Business Server 2003 R2 Premium 32-bit
- Windows Small Business Server 2008 Standard 64-bit
- Windows Small Business Server 2008 Premium 64-bit
- Windows Small Business Server 2011 Standard 64-bit
- Windows Small Business Server 2011 Premium Add-on 64-bit
- Windows Small Business Server 2011 Essentials 64-bit
- Windows Home Server 2011 64-bit
- Windows MultiPoint Server 2010 Standard 64-bit
- Windows MultiPoint Server 2010 Premium 64-bit
- Windows MultiPoint Server 2012 Standard/Premium 64-bit
- Microsoft Windows 2000 Server 32-bit
- Windows Server 2003 Enterprise with Service Pack 2 32-bit/64-bit
- Windows Server 2003 Standard with Service Pack 2 32-bit/64-bit
- Windows Server 2003 R2 Enterprise with Service Pack 2 32-bit/64-bit
- Windows Server 2003 R2 Standard with Service Pack 2 32-bit/64-bit
- Windows Server 2008 Datacenter with Service Pack 1 32-bit/64-bit
- Windows Server 2008 Enterprise with Service Pack 1 32-bit/64-bit

- Windows Server 2008 with Service Pack 1 Server Core 32-bit/64-bit
- Windows Server 2008 Standard with Service Pack 1 32-bit/64-bit
- Windows Server 2008 Standard 32-bit/64-bit
- Windows Server 2008 Enterprise 32-bit/64-bit
- Windows Server 2008 Datacenter 32-bit/64-bit
- Windows Server 2008 R2 Server Core 64-bit
- Windows Server 2008 R2 Datacenter 64-bit
- Windows Server 2008 R2 Enterprise 64-bit
- Windows Server 2008 R2 Foundation 64-bit
- Windows Server 2008 R2 Standard 64-bit
- Windows Server 2016 Nano (Installation Option) (CBB)
- Windows Storage Server 2008 32-bit/64-bit
- Windows Storage Server 2008 with Service Pack 2 64-bit
- Windows Storage Server 2008 R2 64-bit
- Windows Storage Server 2012 64-bit
- Windows Storage Server 2012 R2 64-bit
- Windows Storage Server 2016 64-bit
- Windows Storage Server 2019 64-bit
- Debian GNU/Linux 9.x (Stretch) 32-bit/64-bit
- Debian GNU/Linux 7.x (up to 7.8) 32-bit/64-bit
- Debian GNU/Linux 8.x (Jessie) 32-bit/64-bit
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32-bit/64-bit
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32-bit/64-bit
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64-bit
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-bit/64-bit
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-bit/64-bit
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bit/64-bit
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bit/64-bit

- CentOS 6.x (up to 6.6) 64-bit
- CentOS 7.x ARM 64-bit
- CentOS 8.x 64-bit
- SUSE Linux Enterprise Desktop 12 (all SPs) 64-bit
- SUSE Linux Enterprise Desktop 15 (all Service Packs) 64-bit
- Astra Linux Special Edition 1.5 64-bit
- Astra Linux Special Edition RUSB.10265-01 (operational update 8.1) Elbrus
- Astra Linux Special Edition RUSB.10015-16 (operational update 8.1) Elbrus
- Pardus OS 19.1 64-bit
- Linux Mint 19.x 32-bit
- Lotos (Linux core version 4.19.50, DE: MATE) 64-bit
- ROSA Enterprise Linux Server 7.3 64-bit
- ROSA Enterprise Linux Desktop 7.3 64-bit
- ROSA COBALT Workstation 7.3 64-bit
- ROSA COBALT Server 7.3 64-bit

The following virtualization platforms are not supported:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15

- Microsoft Hyper-V Server 2008 64-bit
- Microsoft Hyper-V Server 2008 R2 64-bit
- Microsoft Hyper-V Server 2008 R2 with Service Pack 1 and later 64-bit
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

Distribution kit

You can purchase the application through online stores of Kaspersky (for example, at <https://www.kaspersky.com>) or through partner companies.

If you purchase Kaspersky Security Center Linux in an online store, you copy the application from the store's website. Information that is required for application activation is sent to you by email after payment.

About compatibility of Administration Server and Kaspersky Security Center Web Console

We recommend that you use the latest version of both Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console. Otherwise, the functionality of Kaspersky Security Center Linux may be limited.

You can install and upgrade Kaspersky Security Center Linux Administration Server and Kaspersky Security Center Web Console independently. In this case you should ensure that the version of the installed Kaspersky Security Center Web Console is compatible with the version of the Administration Server to which you connect:

- Web Console included in Kaspersky Security Center Linux 15 supports Kaspersky Security Center Linux Administration Server of the following versions: 15 and 14.2.
- Administration Server included in Kaspersky Security Center Linux 15 supports Kaspersky Security Center Web Console of the following versions: 15 and 14.2.

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

Kaspersky provides Kaspersky Security Center as an on-premises solution for two platforms—Windows and Linux. In the Windows-based solution, you install Administration Server on a Windows device, and the Linux-based solution has the Administration Server version that is designed to be installed on a Linux device. This Online Help contains information about Kaspersky Security Center Linux. For detailed information about the Windows-based solution, refer to the [Kaspersky Security Center Windows Online Help](#).

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

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

| Feature or property | Kaspersky Security Center 14.2 Windows | Kaspersky Security Center 15 Linux |
|---|--|--|
| Administration Server location | On-premises | On-premises |
| Database management system (DBMS) location | On-premises | On-premises |
| Operating system to install Administration Server on | Windows | Linux |
| Administration console type | On-premises and web-based | Web-based |
| Operating system to install the web-based administration console on | Windows or Linux | Linux |
| Hierarchy of Administration Servers | ✓ | ✓ |
| Administration group hierarchy | ✓ | ✓ |
| Network polling | ✓ | ✓ (by IP ranges and domain controllers, Samba 4 Active Directory, Microsoft Active Directory) |
| Maximum number of managed devices | 100,000 | 50,000 (with PostgreSQL and Postgres Pro) |
| Protection of Windows, macOS, and Linux-managed devices | ✓ | ✓ |
| Protection of mobile devices | ✓ | — |
| Protection of virtual machines | ✓ | ✓ |
| Protection of public cloud infrastructure | ✓ | — |
| Device-centric security management | ✓ | ✓ |
| User-centric security management | ✓ | ✓ |
| Application policies | ✓ | ✓ |
| Tasks for Kaspersky applications | ✓ | ✓ |
| Kaspersky Security Network | ✓ | ✓ |
| KSN Proxy | ✓ | ✓ |
| Kaspersky Private Security Network | ✓ | ✓ |
| Centralized deployment of license keys for Kaspersky applications | ✓ | ✓ |
| Updating anti-virus databases automatically | ✓ | ✓ |
| Support for virtual Administration Servers | ✓ | ✓ |
| Installing third-party software updates and fixing third-party software vulnerabilities | ✓ | — (by using a remote installation task only) |

| | | |
|---|---|---|
| Notifications about events that occurred on managed devices | ✓ | ✓ |
| Creating and managing user accounts | ✓ | ✓ |
| Sign-in to the console by using domain authentication | ✓ | (Single Sign-on is currently not supported) |
| Integration with SIEM systems | ✓ | (by using Syslog only) |
| Monitoring the policies and tasks status | ✓ | ✓ |
| Deployment of the Kaspersky Security Center failover cluster | ✓ | ✓ |
| Installing Administration Server on a Windows Server failover cluster | ✓ | — |
| Using SNMP to send Administration Server statistics to third-party applications | ✓ | — |
| Remote diagnostics of client devices | ✓ | ✓ |
| Remote connection to the desktop of a client device | ✓ | — |
| Managing object revisions | ✓ | — |
| Updating Kaspersky applications automatically | ✓ | — |
| Deployment of operating systems on client devices | ✓ | — |
| Web Server for publishing installation packages and other files | ✓ | — |
| Viewing and working with alerts detected by Kaspersky Endpoint Detection and Response Optimum | ✓ | ✓ |
| Using Administration Server as WSUS server | ✓ | — |
| Integration with Kaspersky Managed Detection and Response | ✓ | — |
| Support for Adaptive Anomaly Control | ✓ | — |
| Support of clusters and server arrays in administration groups | ✓ (in MMC-based Administration Console only) | ✓ |
| Managing third-party licenses | ✓ | — |

About Kaspersky Security Center Cloud Console

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

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

The interface and documentation of Kaspersky Security Center Cloud Console are available in the following languages:

- English
- French
- German
- Italian
- Japanese
- Portuguese (Brazil)
- Russian
- Simplified Chinese
- Spanish
- Spanish (LATAM)
- Traditional Chinese

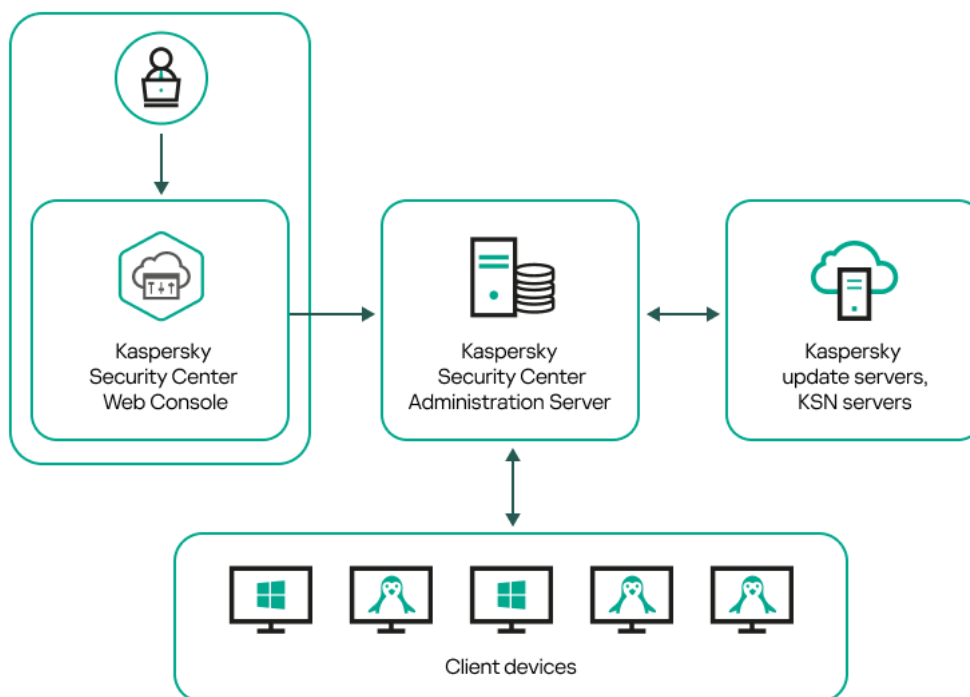
More information [about Kaspersky Security Center Cloud Console](#) and its [features](#) is available in the [Kaspersky Security Center Cloud Console documentation](#) and in the [Kaspersky Endpoint Security for Business documentation](#).

Architecture and basic concepts

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

Architecture

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



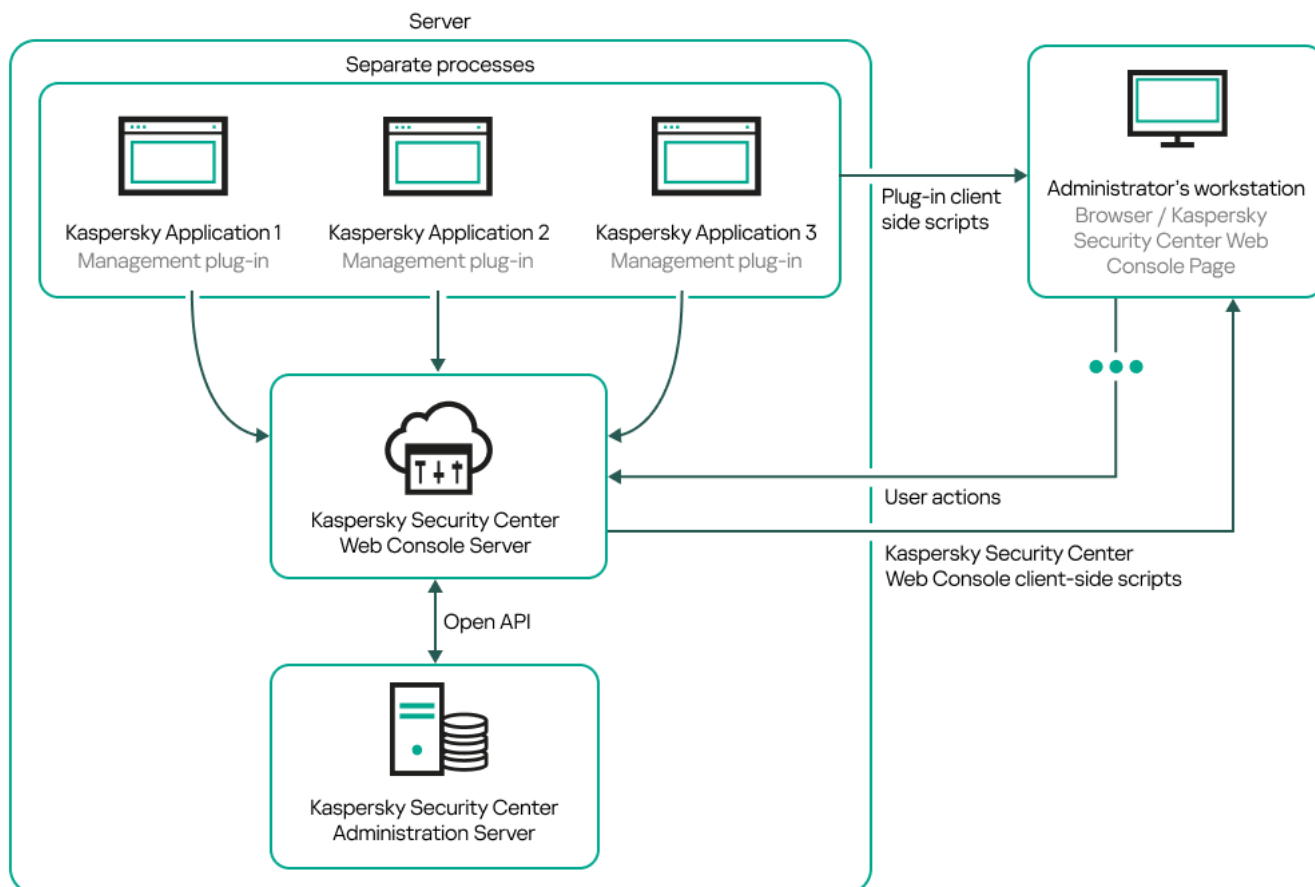
Kaspersky Security Center Linux architecture

Kaspersky Security Center Linux comprises the following main components:

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

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

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



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

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

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

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

Ports used by Kaspersky Security Center Linux

The tables below show the default ports that must be open on Administration Server and on client devices. If you want, you can change each of these default port numbers.

Ports used by Kaspersky Security Center Linux Administration Server

| Port | Name of | Protocol | Port purpose | Scope |
|------|---------|----------|--------------|-------|
|------|---------|----------|--------------|-------|

| number | the process that opens the port | | | |
|---|---------------------------------|-----------|--|--|
| 8060 | klcsweb | TCP | Transmitting published installation packages to client devices | Publishing installation packages. You can change the default port number in the Web Server section of the Administration Server properties window. |
| 8061 | klcsweb | TCP (TLS) | Transmitting published installation packages to client devices | Publishing installation packages. You can change the default port number in the Web Server section of the Administration Server properties window. |
| 13000 | klserver | TCP (TLS) | Receiving connections from Network Agents and secondary Administration Servers; also used on secondary Administration Servers for receiving connections from the primary Administration Server (for example, if the secondary Administration Server is in DMZ) | Managing client devices and secondary Administration Servers. You can change the number of the default port for receiving connections from Network Agents when configuring connection ports during the installation of Kaspersky Security Center Linux; you can change the number of default port for receiving connections from secondary Administration Servers when creating a hierarchy of Administration Servers . |
| 13000 | klserver | UDP | Receiving information about devices that were turned off from Network Agents | Managing client devices. You can change the default port number in the Network Agent policy settings . |
| 13299 | klserver | TCP (TLS) | Receiving connections from Kaspersky Security Center Web Console to the Administration Server; receiving connections to the Administration Server over OpenAPI | Kaspersky Security Center Web Console, OpenAPI. You can change the default port number in the Administration Server properties window (in the Connection ports subsection of the General section), or when creating a hierarchy of Administration Servers . |
| 14000 | klserver | TCP | Receiving connections from Network Agents | Managing client devices. You can change the default port number when configuring connection ports during the installation of Kaspersky Security Center Linux, or when manually connecting a client device to the Administration Server . |
| 13111 (only if KSN proxy service is run on the device) | ksnproxy | TCP | Receiving requests from managed devices to KSN proxy server | KSN proxy server. You can change the default port number in the Administration Server properties window . |
| 15111 | ksnproxy | UDP | Receiving requests from | KSN proxy server. |

| | | | | |
|--|----------|-------------|---|--|
| (only if KSN proxy service is run on the device) | | | managed devices to KSN proxy server | You can change the default port number in the Administration Server properties window . |
| 17000 | klactprx | TCP (TLS) | Receiving connections for application activation from managed devices | Activation proxy server for managed devices. You can change the default port number in the Administration Server properties window (in the Additional ports subsection of the General section). |
| 19170 | klserver | HTTPS (TLS) | Tunneling connections to managed devices by using the klsc tunnel utility | Remotely connecting to managed devices by using Kaspersky Security Center Web Console. You can change the default port number by using the klscflag utility. |

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

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

Port used by Kaspersky Security Center Web Console Server

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

The table below shows the port that must be open on managed devices where Network Agent is installed.

Ports used by Network Agent

| Port number | Name of the process that opens the port | Protocol | Port purpose | Scope |
|-------------|---|----------|---|---|
| 15000 | klagent | UDP | Management signals from Administration Server or distribution point to Network Agents | Managing client devices. You can change the default port number in the Network Agent policy settings . |

| | | | | |
|-------|---------|---------------|--|--|
| 15000 | klagent | UDP broadcast | Getting data about other Network Agents within the same broadcasting domain (the data is then sent to the Administration Server) | Delivering updates and installation packages. |
| 15001 | klagent | UDP | Receiving multicast requests from a distribution point (if in use) | Receiving updates and installation packages from a distribution point. You can change the default port number in the distribution point properties window . |

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

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

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

Ports used by Network Agent functioning as distribution point

| Port number | Name of the process that opens the port | Protocol | Port purpose | Scope |
|--|---|-----------|---|---|
| 13000 | klagent | TCP (TLS) | Receiving connections from Network Agents and connection gateways | Managing client devices, delivering updates and installation packages. You can change the default port number in the distribution point properties . |
| 13111 (only if KSN proxy service is run on the device) | ksnproxy | TCP | Receiving requests from managed devices to KSN proxy server | KSN proxy server. You can change the default port number in the distribution point properties . |
| 15111 (only if KSN proxy service is run on the device) | ksnproxy | UDP | Receiving requests from managed devices to KSN proxy server | KSN proxy server. You can change the default port number in the distribution point properties . |

Ports used by Kaspersky Security Center Web Console

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

Ports used by Kaspersky Security Center Web Console

| Port number | Service name | Protocol | Port purpose | Scope |
|------------------|--------------------------------|----------|---|---|
| 2001 | KSCWebConsolePlugin | HTTPS | API port that is used by the management plug-in processes to receive requests from the KSCWebConsoleManagementService | Running node process manage plug-ins |
| 1329, 2003 | KSCWebConsoleManagementService | HTTPS | API ports that are used to receive requests from the KSCWebConsoleManagementService running on the same device | Updating Kaspers Security Center Web Console component |
| 2005 | KSCWebConsole | HTTPS | API port that is used to receive requests from the KSCWebConsoleManagementService service running on the same device | Running node process Kaspers Security Center Web Console |
| 8200 | — | HTTP | API port that is used to generate certificates by means of HashiCorp Vault (for more details, see the HashiCorp Vault website) | Installing Kaspers Security Center Web Console updating Kaspers Security Center Web Console component |
| 4150, 4151, 4152 | KSCWebConsoleMessageQueue | HTTPS | API ports of the Message Broker that are used for communication between processes of both Kaspersky Security Center Web Console and management plug-ins | Interact between Kaspers Security Center Web Console manage plug-ins |

Basic concepts

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

Administration Server

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

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

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

- With the name "Kaspersky Security Center Administration Server"
- Set to start automatically when the operating system starts
- With the **LocalSystem** account or the user account selected during the installation of Administration Server

Administration Server performs the following functions:

- Storage of the administration groups' structure
- Storage of information about the configuration of client devices
- Organization of repositories for application distribution packages
- Remote installation of applications to client devices and removal of applications
- Updating application databases and software modules of Kaspersky applications
- Management of policies and tasks on client devices
- Storage of information about events that have occurred on client devices
- Generation of reports on the operation of Kaspersky applications
- Deployment of license keys to client devices and storing information about the license keys
- Forwarding notifications about the progress of tasks (such as detection of viruses on a client device)

Naming Administration Servers in the application interface

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

- Name of the Administration Server device, for example: "*device_name*" or "Administration Server: *device_name*".
- IP address of the Administration Server device, for example: "*IP_address*" or "Administration Server: *IP_address*".
- Secondary Administration Servers and virtual Administration Servers have custom names that you specify when you connect a virtual or a secondary Administration Server to the primary Administration Server.

- If you use Kaspersky Security Center Web Console installed on a Linux device, the application displays the names of the Administration Servers that you specified as trusted in the [response file](#).

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

Hierarchy of Administration Servers

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

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

[Virtual Administration Servers](#) are a particular case of secondary Administration Servers.

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

- Decrease the load on Administration Server (compared to a single installed Administration Server for an entire network).
- Decrease intranet traffic and simplify work with remote offices. You do not have to establish connections between the primary Administration Server and all networked devices, which may be located, for example, in different regions. It is sufficient to install a secondary Administration Server in each network segment, distribute devices among administration groups of secondary Servers, and establish connections between the secondary Servers and the primary Server over fast communication channels.
- Distribute responsibilities among the anti-virus security administrators. All capabilities for centralized management and monitoring of the anti-virus security status in corporate networks remain available.
- Use Kaspersky Security Center by service providers. The service provider only needs to install Kaspersky Security Center and Kaspersky Security Center Web Console. To manage a large number of client devices of various organizations, a service provider can add secondary Administration Servers (including virtual Servers) to the hierarchy of Administration Servers.

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

Virtual Administration Server

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

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

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

In addition, virtual Administration Server has the following restrictions:

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

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

Web Server

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

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

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

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

The syntax of the information transfer link is as follows:

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

where:

- <Web Server name> is the name of Kaspersky Security Center Web Server.

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

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

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

Network Agent

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

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

- With 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 from one of the following sources:

- Installation package in Administration Server storage (you must have Administration Server installed)
- Installation package located at Kaspersky web servers

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

The names of the process that Network Agent starts are as follows:

- `klagent64.service` (for a 64-bit operating system)
- `klagent.service` (for a 32-bit operating system)

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

Administration groups

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

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

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

A managed device can belong to only one administration group.

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

Managed device

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

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

A device can be managed by only one Administration Server. One Administration Server can manage up to 20,000 devices.

Unassigned device

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

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

Administrator's workstation

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

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

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

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

Management web plug-in

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

You can download management web plug-ins from the [Kaspersky Technical Support webpage](#).

The management plug-in provides the following:

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

Policies

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

The status of the policy

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

Policies function according to the following rules:

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

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

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

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

Policy profiles function according to the following rules:

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

Policy profiles

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

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

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

Tasks

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

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

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

The following tasks are performed on the Administration Server:

- Automatic distribution of reports
- Downloading of updates to the repository of the Administration Server
- Backup of Administration Server data
- Maintenance of the database
- Creation of an installation package based on the operating system (OS) image of a reference device

The following types of tasks are performed on devices:

- *Local tasks*—Tasks that are performed on a specific device
Local tasks can be modified either by the administrator, by using Kaspersky Security Center Web Console, or by the user of a remote device (for example, through the security application interface). If a local task has been modified simultaneously by the administrator and the user of a managed device, the changes made by the administrator will take effect because they have a higher priority.
- *Group tasks*—Tasks that are performed on all devices of a specific group
Unless otherwise specified in the task properties, a group task also affects all subgroups of the selected group. A group task also affects (optionally) devices that have been connected to secondary and virtual Administration Servers deployed in the group or any of its subgroups.
- *Global tasks*—Tasks that are performed on a set of devices, regardless of whether they are included in any group

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

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

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

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

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

Task scope

The *scope of a [task](#)* is the set of devices on which the task is performed. The types of scope are as follows:

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

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

- Specifying certain devices manually.

You can use an IP address (or IP range) or DNS name as the device address.

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

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

- Specifying a device selection.

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

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

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

How local application settings relate to policies

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

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

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

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

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

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

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

Distribution point

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

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

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

- Distribute policies and group tasks through multicasting using UDP.
- Act as a gateway for connection to the Administration Server for devices in an administration group.
If a direct connection between managed devices within the group and the Administration Server cannot be established, you can use the distribution point as a connection gateway to the Administration Server for this group. In this case, managed devices connect to the connection gateway, which in turn connects to the Administration Server.

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

- Poll the network to detect new devices and update information about existing ones. A distribution point can apply the same device discovery methods as the Administration Server.
- Perform remote installation of applications by Kaspersky and other software vendors, including installation on client devices without Network Agent.

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

- Act as a proxy server participating in Kaspersky Security Network (KSN).
You can [enable KSN proxy server on distribution point side](#) to make the device act as a KSN proxy server. In this case, the [KSN proxy service is run on the device](#).

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

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

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

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

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

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

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

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

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

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

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

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

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

Connection gateway

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

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

You have two options for using connection gateways:

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

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

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

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

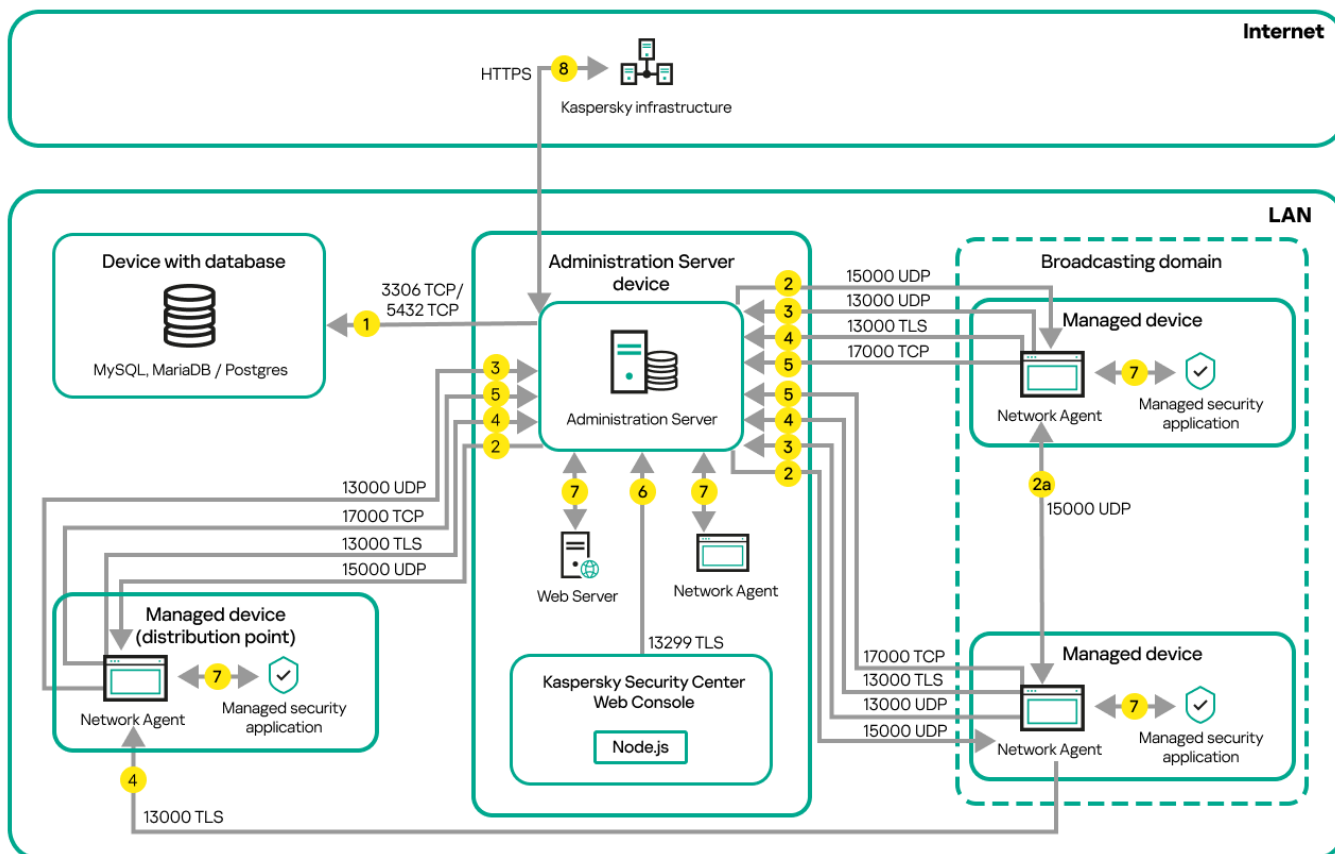
- You can also use connection gateways within the network. For example, automatically assigned distribution points also become connection gateways in their own scope. However, within an internal network, connection gateways do not provide considerable benefit. They reduce the number of network connections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

Schemas for data traffic and port usage

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

Administration Server and managed devices on LAN

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



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

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

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

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

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

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

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

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

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

4. The Administration Server receives connection [from Network Agents](#) and [from secondary Administration Servers](#) through SSL port 13000.

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

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

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

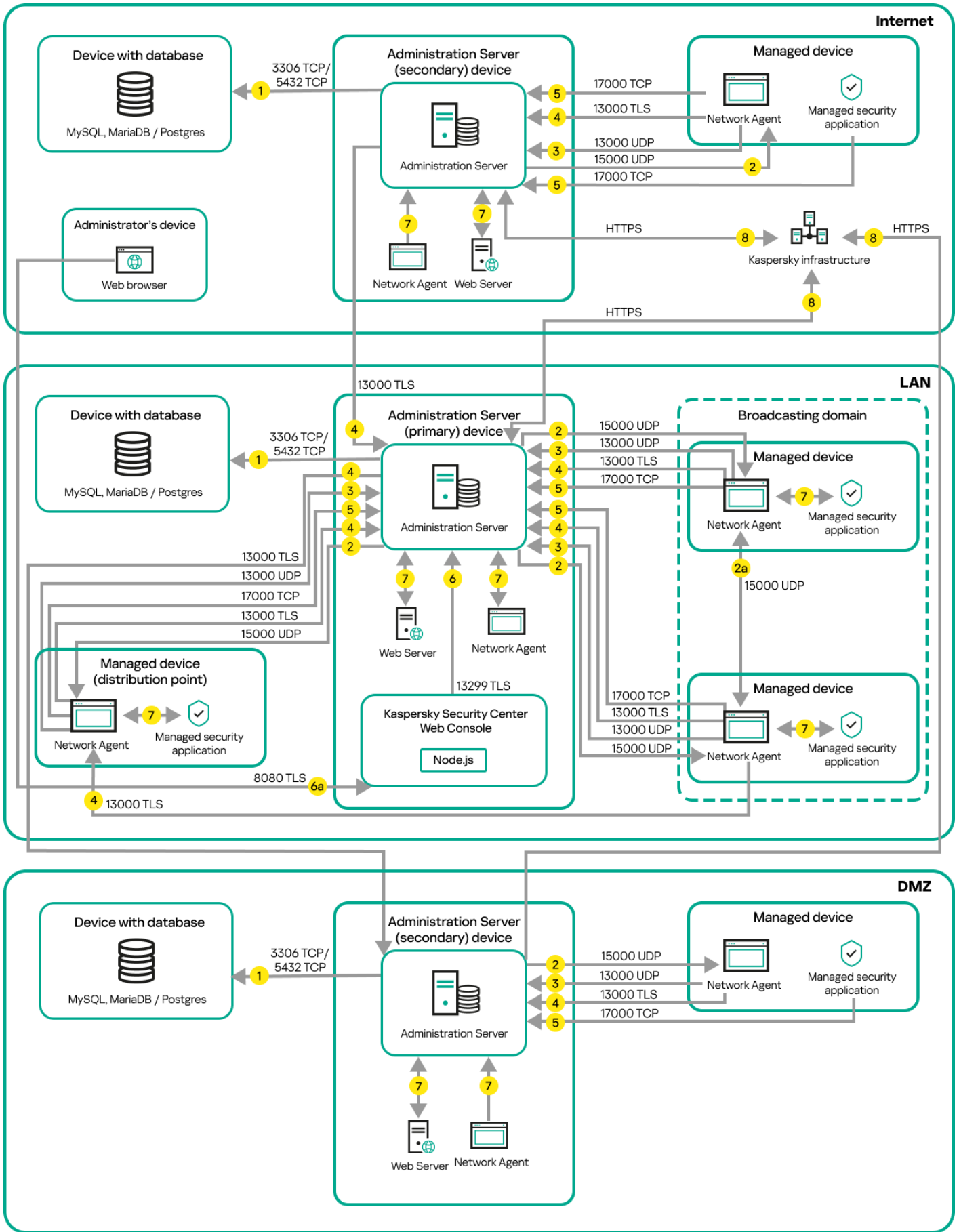
7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.

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

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

Primary Administration Server on LAN and two secondary Administration Servers

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



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

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

1. [Administration Server sends data to the database](#). If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 5432 for PostgreSQL Server or Postgres Pro Server). Please refer to the DBMS documentation for the relevant information.
2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through [UDP port 15000](#).

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

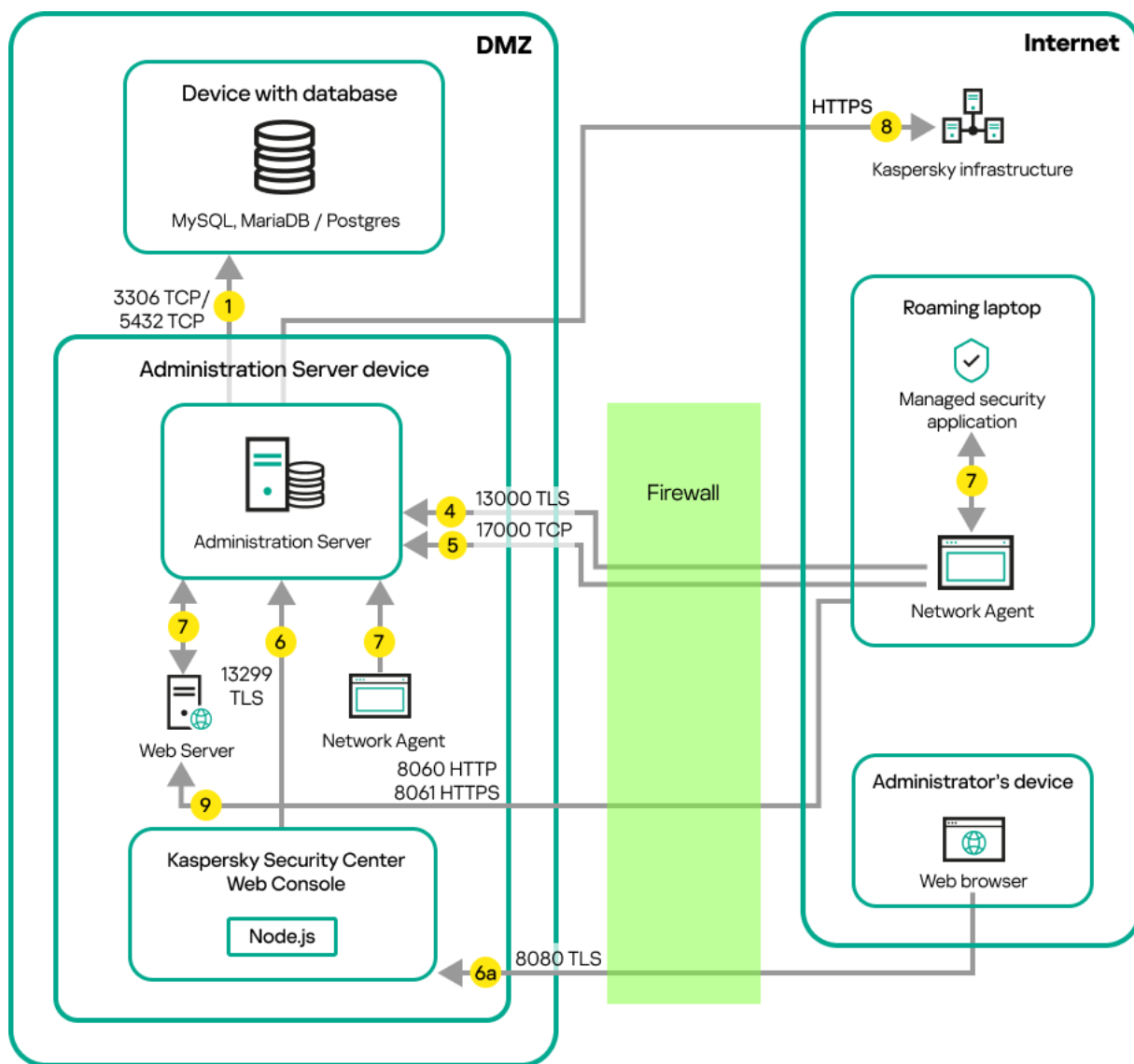
If Administration Server does not have direct access to the managed devices, communication requests from Administration Server to these devices are not sent directly.
3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.
4. The Administration Server receives connection [from Network Agents](#) and [from secondary Administration Servers](#) through SSL port 13000.

If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-SSL port 14000. Kaspersky Security Center Linux also supports connection of Network Agents through port 14000, although using SSL port 13000 is recommended.
5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the internet; in this case, the device sends the data to Kaspersky servers over the internet directly.
6. Kaspersky Security Center Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.
 - 6a. Data from the browser, which is installed on a separate device of the administrator, is transferred to Kaspersky Security Center Web Console Server [through TLS port 8080](#). The Kaspersky Security Center Web Console Server can be installed either on the Administration Server or on another device.
7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.
8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.

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

Administration Server on LAN, managed devices on internet, firewall in use

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



Administration Server on a local area network; managed devices connect to the Administration Server through a corporate firewall

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

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

- Administration Server sends data to the database. If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 5432 for PostgreSQL Server or Postgres Pro Server). Please refer to the DBMS documentation for the relevant information.
- Requests for communication from the Administration Server are transferred to all non-mobile managed devices through UDP port 15000.
 Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).
 If Administration Server does not have direct access to the managed devices, communication requests from Administration Server to these devices are not sent directly.
- Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.

4. The Administration Server receives connection [from Network Agents](#) and [from secondary Administration Servers](#) through SSL port 13000.

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

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

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

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

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

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

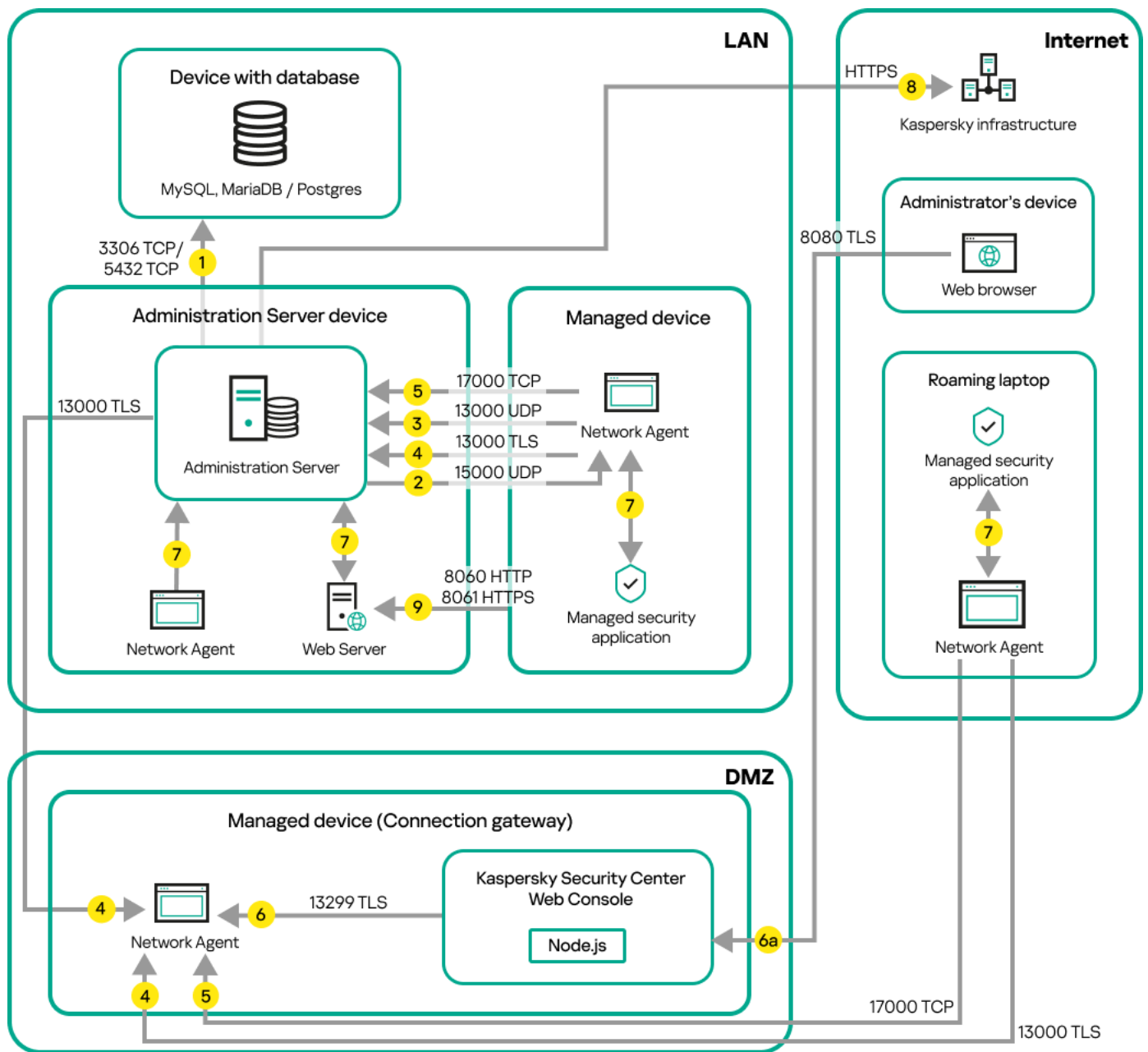
If you do not want your Administration Server to have access to the internet, you must manage this data manually.

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

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

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

This deployment scheme is recommended if you do not want the managed devices to connect to the Administration Server directly and do not want to use a Microsoft Forefront Threat Management Gateway (TMG) or corporate firewall.



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

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

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

1. [Administration Server sends data to the database.](#) If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 5432 for PostgreSQL Server or Postgres Pro Server). Please refer to the DBMS documentation for the relevant information.
2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through [UDP port 15000](#).

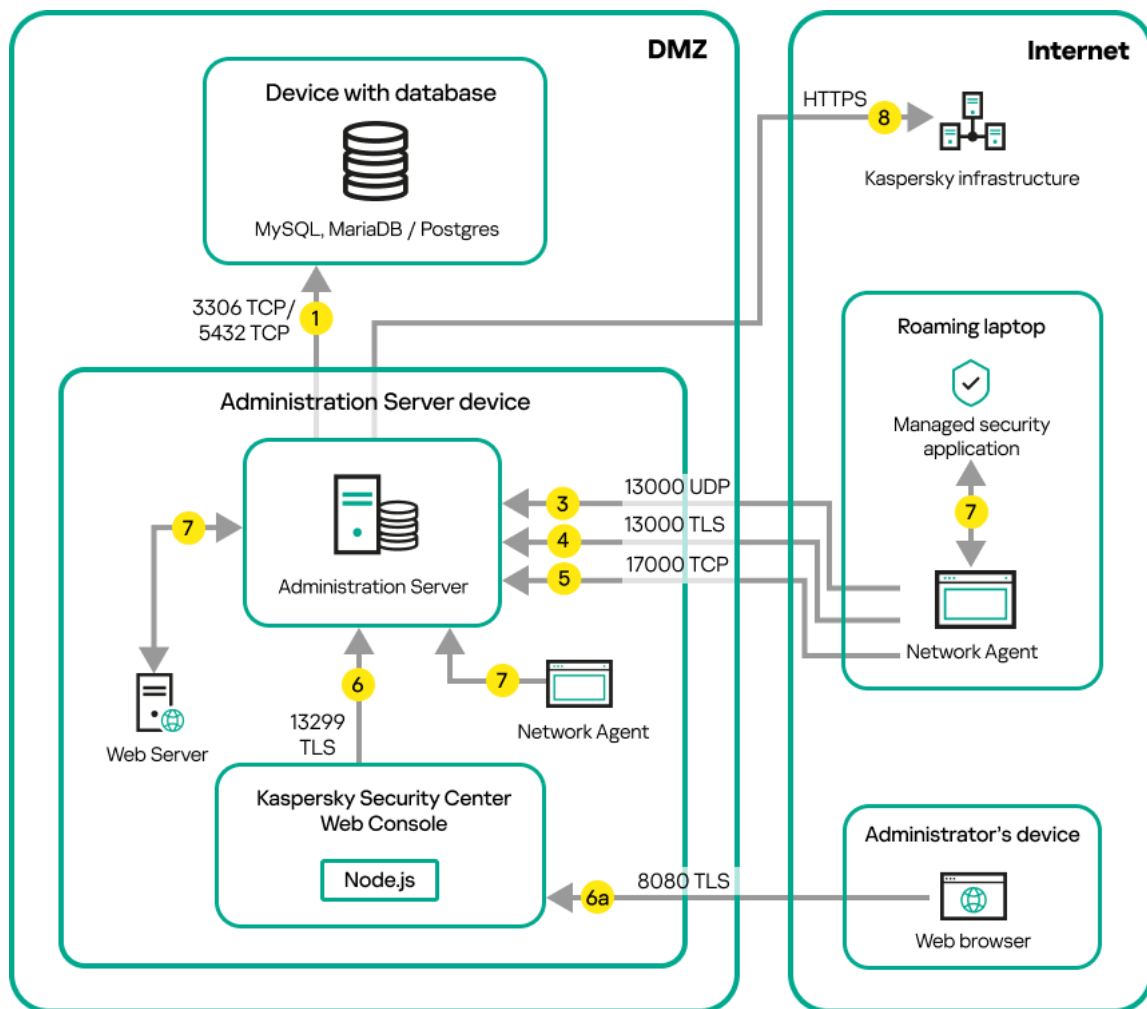
Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).

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

3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.
4. The Administration Server receives connection [from Network Agents](#) and [from secondary Administration Servers](#) through SSL port 13000.
If you used an earlier version of Kaspersky Security Center, the Administration Server on your network can receive connection from Network Agents through non-SSL port 14000. Kaspersky Security Center Linux also supports connection of Network Agents through port 14000, although using SSL port 13000 is recommended.
5. The managed devices (except for mobile devices) request activation through TCP port 17000. This is not necessary if the device has its own access to the internet; in this case, the device sends the data to Kaspersky servers over the internet directly.
6. Kaspersky Security Center Web Console Server sends data to the Administration Server, which may be installed on the same or on a different device, through TLS port 13299.
 - 6a. Data from the browser, which is installed on a separate device of the administrator, is transferred to Kaspersky Security Center Web Console Server [through TLS port 8080](#). The Kaspersky Security Center Web Console Server can be installed either on the Administration Server or on another device.
7. Applications on a single device exchange local traffic (either on the Administration Server or on a managed device). No external ports have to be opened.
8. Data from the Administration Server to the Kaspersky servers (such as KSN data or information about licenses) and data from the Kaspersky servers to the Administration Server (such as application updates and anti-virus database updates) are transferred using the HTTPS protocol.
If you do not want your Administration Server to have access to the internet, you must manage this data manually.
9. Requests for packages from managed devices, including mobile devices, are transferred to the [Web Server](#), which is on the same device as the Administration Server.

Administration Server in DMZ, managed devices on internet

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



Administration Server in DMZ, managed mobile devices on the internet

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

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

1. [Administration Server sends data to the database](#). If you install the Administration Server and the database on different devices, you must make available the necessary ports on the device where the database is located (for example, port 3306 for MySQL Server and MariaDB Server, or port 5432 for PostgreSQL Server or Postgres Pro Server). Please refer to the DBMS documentation for the relevant information.
2. Requests for communication from the Administration Server are transferred to all non-mobile managed devices through [UDP port 15000](#).
Network Agents send requests to each other within one broadcasting domain. The data is then sent to the Administration Server and is used for defining the limits of the broadcasting domain and for automatic assignment of distribution points (if this option is enabled).
If Administration Server does not have direct access to the managed devices, communication requests from Administration Server to these devices are not sent directly.
3. Information about shutdown of the managed devices is transferred from Network Agent to the Administration Server through UDP port 13000.
4. The Administration Server receives connection [from Network Agents](#) and [from secondary Administration Servers](#) through SSL port 13000.

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

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

Out-of-office devices connect to the connection gateway through [SSL port 13000](#) as well.

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

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

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

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

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

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

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


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













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

Conventions used in interaction schemas

The following table provides the conventions used across the schemas.

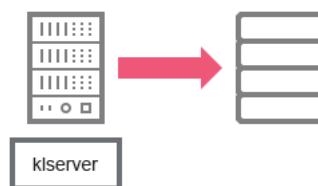
Document conventions

| Icon | Meaning |
|---|-----------------------|
|  | Administration Server |

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

Administration Server and DBMS

Data from the Administration Server enter a [database](#).

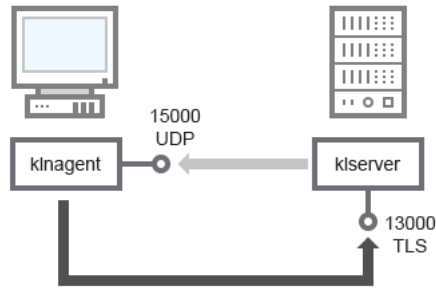


Administration Server and DBMS

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

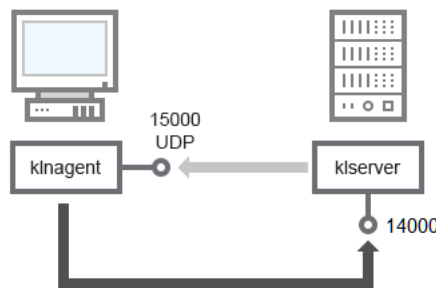
Administration Server and client device: Managing the security application

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



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

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



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

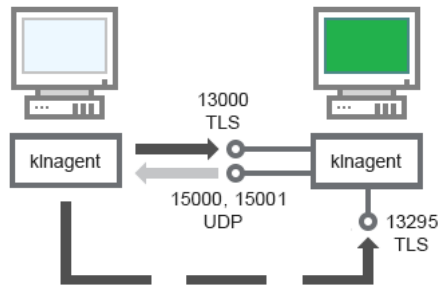
For clarifications of schemas, see the table below.

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

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

Upgrading software on a client device through a distribution point

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



Upgrading software on a client device through a distribution point

For schema clarifications, see the table below.

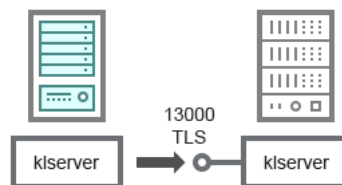
Upgrading software through a distribution point (traffic)

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

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

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

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



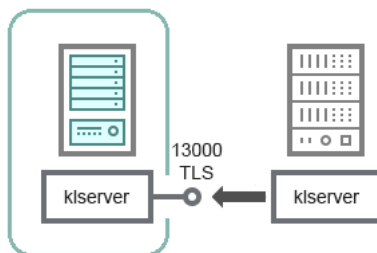
Hierarchy of Administration Servers: primary Administration Server and secondary Administration Server

For schema clarifications, see the table below.

Hierarchy of Administration Servers (traffic)

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

Hierarchy of Administration Servers with a secondary Administration Server in DMZ



Hierarchy of Administration Servers with a secondary Administration Server in DMZ

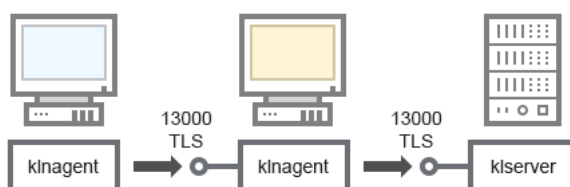
The schema shows a hierarchy of Administration Servers in which the secondary Administration Server located in DMZ receives a connection from the primary Administration Server (see the table below for schema clarifications). When combining two Administration Servers into a hierarchy, make sure that port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

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

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

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

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



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

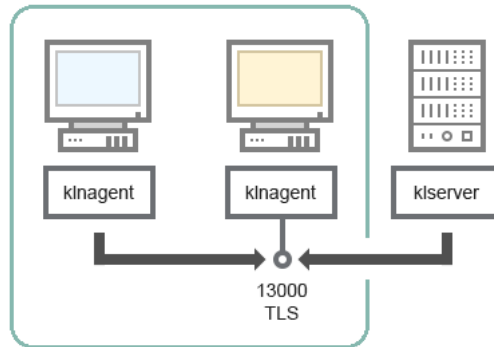
For schema clarifications, see the table below.

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

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

| | | | | |
|---------------|-------|---------|-----------|---|
| Network Agent | 13000 | klagent | TCP (TLS) | Receiving connections from Network Agents |
|---------------|-------|---------|-----------|---|

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



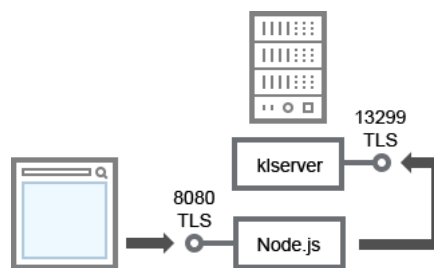
Administration Server with a connection gateway and a client device in DMZ

For schema clarifications, see the table below.

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

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

Administration Server and Kaspersky Security Center Web Console



Administration Server and Kaspersky Security Center Web Console

For schema clarifications, see the table below.

Administration Server and Kaspersky Security Center Web Console (traffic)

| Device | Port number | Name of the process that opens the port | Protocol | Port purpose |
|-----------------------|-------------|---|-----------|--|
| Administration Server | 13299 | klservice | TCP (TLS) | Receiving connections from Kaspersky Security Center Web Console to the Administration Server over OpenAPI |

| | | | | |
|---|------|---------------------------------------|--------------|--|
| Kaspersky Security Center Web Console Server or Administration Server | 8080 | Node.js: Server-side JavaScript | TCP (TLS) | Receiving connections from Kaspersky Security Center Web Console |
|---|------|---------------------------------------|--------------|--|

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

Getting started

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

Prerequisites

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

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

Stages

The main installation scenario proceeds in stages:

1 Selecting a structure for protection of an organization

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

Define whether a [hierarchy of Administration Servers](#) will be used in your organization. To do this, you must evaluate whether it is possible and expedient to cover all client devices with a single Administration Server or it is necessary to build a hierarchy of Administration Servers. You may also have to build a hierarchy of Administration Servers that is identical to the organizational structure of the organization whose network you want to protect.

2 Preparation for the use of custom certificates

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

3 Installing a database management system (DBMS)

Install the DBMS that will be used by Kaspersky Security Center Linux or use an existing one.

You can choose from one of the [supported DBMSs](#). For information about how to install the selected DBMS, refer to its documentation.

If the distribution of your Linux-based operating system does not contain a supported DBMS, you can install the DBMS from a third-party package repository. If installing distributions from third-party repositories is prohibited, you can install the DBMS on a separate device.

If you decide to install PostgreSQL or Postgres Pro DBMS, ensure that you specified a password for the superuser. If the password is not specified, Administration Server might not be able to connect to the database.

If you install [MariaDB](#), [PostgreSQL](#), or [Postgres Pro](#), use the recommended settings to ensure the DBMS functions properly.

If you want to change the [DBMS type](#) after the installation, you have to reinstall Kaspersky Security Center Linux. The data can be partially and manually transferred to another database.

4 Configuring ports

Make sure that all the necessary [ports](#) are open for interaction between components in accordance with your selected security structure.

If you have to provide [internet access to the Administration Server](#), configure the ports and specify the connection settings, depending on the network configuration.

5 Installing Kaspersky Security Center Linux

Select a Linux device that you intend to use as Administration Server, ensure that the device meets the [software and hardware requirements](#), and then [install Kaspersky Security Center Linux](#) on the device. The server version of Network Agent is installed together with Administration Server automatically.

6 Installing Kaspersky Security Center Web Console and management web plug-ins

Select a Linux device that you intend to use as the administrator's workstation, ensure that the device meets the [software and hardware requirements](#), and then install Kaspersky Security Center Web Console on the device. You can install Kaspersky Security Center Web Console either on the same device where Administration Server is installed or on another device.

[Download the Kaspersky Endpoint Security for Linux management web plug-in](#) and then install it on the same device where Kaspersky Security Center Web Console is installed.

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

By default, the application does not consider the Administration Server device as a managed device. To protect Administration Server against viruses and other threats, and to manage the device as any other managed device, we recommend that you [install Kaspersky Endpoint Security for Linux](#) and [Network Agent for Linux](#) on the Administration Server device. In this case, Network Agent for Linux is installed and works independently from the server version of Network Agent that you installed together with Administration Server.

8 Performing initial setup

When Administration Server installation is complete, the first connection to the Administration Server the [quick start wizard](#) starts automatically. Perform initial configuration of Administration Server according to the existing requirements. During the initial configuration stage, the wizard uses the default settings to create the [policies](#) and [tasks](#) that are required for protection deployment. However, the default settings may be less than optimal for the needs of your organization. If necessary, you can [edit the settings of policies and tasks](#).

9 Discovery of networked devices

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

10 Arranging devices into administration groups

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

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

11 Assigning distribution points

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

12 Installing Network Agent and security applications on networked devices

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

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

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

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

13 Deploying license keys to client devices

Deploy [license keys](#) to client devices to activate managed security applications on those devices.

14 Configuring Kaspersky application policies

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

15 Monitoring the network protection status

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

Installation

This section describes installation of Kaspersky Security Center Linux and Kaspersky Security Center Web Console.

Configuring the MariaDB x64 server for working with Kaspersky Security Center Linux

Recommended settings for the my.cnf file

For more details about DBMS configuring, refer also to the [account configuring](#) procedure. For information about DBMS installation, refer to the [DBMS installation](#) procedure.

To configure the my.cnf file:

1. [Open the my.cnf file](#) in a text editor.
2. Enter the following lines into the [mysqld] section of the my.cnf file:

```
sort_buffer_size=10M  
join_buffer_size=100M  
join_buffer_space_limit=300M  
join_cache_level=8  
tmp_table_size=512M
```

```
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=< value >
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

The value of the `innodb_buffer_pool_size` must be no less than 80 percent of the expected KAV database size. Note that the specified memory is allocated at server startup. If the database size is smaller than the specified buffer size, only the required memory is allocated. If you use MariaDB 10.4.3 or older, the actual size of allocated memory is approximately 10 percent greater than the specified buffer size.

It is recommended to use the parameter value `innodb_flush_log_at_trx_commit=0`, because the values "1" or "2" negatively affect the operating speed of MariaDB.

By default, the optimizer add-ons `join_cache_incremental`, `join_cache_hashed`, `join_cache_bka` are enabled. If these add-ons are not enabled, you must enable them.

To check whether optimizer add-ons are enabled:

1. In the MariaDB client console, execute the command:

```
SELECT @@optimizer_switch;
```

2. Make sure that its output contains the following lines:

```
join_cache_incremental=on
join_cache_hashed=on
join_cache_bka=on
```

If these lines are present and have the values `on`, then optimizer add-ons are enabled.

If these lines are missing or have `off` values, you need to do the following:

a. Open the `my.cnf` file in a text editor.

b. Add the following lines into the `my.cnf` file:

```
optimizer_switch='join_cache_incremental=on'
optimizer_switch='join_cache_hashed=on'
optimizer_switch='join_cache_bka=on'
```

The add-ons `join_cache_incremental`, `join_cache_hash`, and `join_cache_bka` are enabled.

Configuring the PostgreSQL or Postgres Pro server for working with Kaspersky Security Center Linux

Kaspersky Security Center Linux supports PostgreSQL and Postgres Pro DBMSs. If you use one of these DBMSs, consider configuring the DBMS server parameters to optimize the DBMS work with Kaspersky Security Center Linux.

The default path to the configuration file is: `/etc/postgresql/< VERSION >/main/postgresql.conf`

Recommended parameters for PostgreSQL and Postgres Pro:

- `shared_buffers` = 25% of the RAM value of the device where the DBMS is installed
If RAM is less than 1 GB, then leave the default value.
- `max_stack_depth` = maximum stack size (execute the `'ulimit -s'` command to obtain this value in KB) minus the 1 MB safety margin
- `temp_buffers` = 24MB
- `work_mem` = 16MB
- `max_connections` = 151
- `max_parallel_workers_per_gather` = 0
- `maintenance_work_mem` = 128 MB

Restart or reload the server after updating the `postgresql.conf` file to apply changes. Refer to the [PostgreSQL documentation](#) for details.

Refer to the following topic for details on how to create and configure accounts for PostgreSQL and Postgres Pro: [Configuring accounts for work with PostgreSQL and Postgres Pro](#).

For detailed information about PostgreSQL and Postgres Pro server parameters and on how to specify the parameters, refer to the corresponding DBMS documentation.

Scenario: Authenticating PostgreSQL Server

We recommend that you use a TLS certificate to authenticate the PostgreSQL server. You can use a certificate from a trusted certification authority (CA) or a self-signed certificate. Use a certificate from a trusted CA because a self-signed certificate provides only limited protection.

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

Follow these steps to configure SSL authentication for PostgreSQL:

1 Generate a certificate for the PostgreSQL server.

Run the following commands:

```
openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj  
"/CN=psql"
```

```
chmod og-rwx psql.key
```

2 Generate a certificate for the Administration Server.

Run the following commands. The CN value should match the name of the user that connects to PostgreSQL on behalf of the Administration Server. The username is set to `postgres` by default.

```
openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -  
subj "/CN=postgres"
```

```
chmod og-rwx postgres.key
```

3 Configure client certificate authentication.

Modify pg_hba.conf as follows:

```
hostssl all all 0.0.0.0/0 md5
```

Ensure that pg_hba.conf doesn't include a record that starts with host.

4 Specify the PostgreSQL certificate.

[One-way SSL authentication](#)

Modify postgresql.conf as follows (specify the correct path to the .crt and .key files):

```
listen_addresses = '*'
ssl = on
ssl_cert_file = 'psql.crt'
ssl_key_file = 'psql.key'
```

[Two-way SSL authentication](#)

Modify postgresql.conf as follows (specify the correct path to the .crt and .key files):

```
listen_addresses = '*'
ssl = on
ssl_ca_file = '<postgres.crt>'
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

5 Restart the PostgreSQL daemon.

Run the following command:

```
systemctl restart postgresql-14.service
```

6 Specify the server flag for the Administration Server.

[One-way SSL authentication](#)

Navigate to the ServerFlags directory and create a file that corresponds to the KLSRV_POSTGRES_OPT_SSL_CA server flag:

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
mkfile KLSRV_POSTGRES_OPT_SSL_CA
```

In the created file, specify the path to the psql.crt file.

[Two-way SSL authentication](#)

Navigate to the ServerFlags directory and create files that correspond to the server flags:

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/  
mkfile KLSRV_POSTGRES_OPT_SSL_CA  
mkfile KLSRV_POSTGRES_OPT_SSL_CERT  
mkfile KLSRV_POSTGRES_OPT_SSL_KEY
```

Edit the created files as follows:

- KLSRV_POSTGRES_OPT_SSL_CA: specify the path to the psql.crt file.
- KLSRV_POSTGRES_OPT_SSL_CERT: specify the path to the postgres.crt file.
- KLSRV_POSTGRES_OPT_SSL_KEY: specify the path to the postgres.key file.

If the postgres.key requires a passphrase, create a KLSRV_POSTGRES_OPT_TLS_PASPHRASE file in the ServerFlags folder and specify the passphrase in it.

7 Restart the Administration Server service.

Scenario: Authenticating MySQL Server

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

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

Enable one-way SSL authentication

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

1. Navigate to the ServerFlags directory and create a file that corresponds to the KLSRV_MYSQL_OPT_SSL_CA server flag:

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/  
mkfile KLSRV_MYSQL_OPT_SSL_CA
```

2. In the KLSRV_MYSQL_OPT_SSL_CA file, specify the path to the certificate (the ca-cert.pem file).

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

```
[mysqld]  
ssl-ca="C:/mysqlCerts/ca-cert.pem"  
ssl-cert="C:/mysqlCerts/server-cert.pem"  
ssl-key="C:/mysqlCerts/server-key.pem"
```

Enable two-way SSL authentication

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

1. Navigate to the ServerFlags directory and create files that correspond to the server flags:

```
cd /etc/opt/kaspersky/klagent_srv/1093/1.0.0.0/ServerFlags/  
mkfile KLSRV_MYSQL_OPT_SSL_CA  
mkfile KLSRV_MYSQL_OPT_SSL_CERT  
mkfile KLSRV_MYSQL_OPT_SSL_KEY
```

2. Edit the created files as follows:

KLSRV_MYSQL_OPT_SSL_CA: specify the path to the ca-cert.pem file.

KLSRV_MYSQL_OPT_SSL_CERT: specify the path to the server-cert.pem file.

KLSRV_MYSQL_OPT_SSL_KEY: specify the path to the server-key.pem file.

If the server-key.pem requires a passphrase, create a KLSRV_MARIADB_OPT_TLS_PASPHRASE file in the ServerFlags folder and specify the passphrase in it.

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

```
[mysqld]  
ssl-ca="C:/mysqlCerts/ca-cert.pem"  
ssl-cert="C:/mysqlCerts/server-cert.pem"  
ssl-key="C:/mysqlCerts/server-key.pem"
```

Installing Kaspersky Security Center Linux

This procedure describes how to install Kaspersky Security Center Linux.

Before installation:

- [Install a DBMS.](#)
- Make sure that the device on which you want to install Kaspersky Security Center Linux is running one of the [supported Linux distributions.](#)

Use the installation file—ksc64_[version_number]_amd64.deb or ksc64-[version_number].x86_64.rpm—that corresponds to the Linux distribution installed on your device. You receive the installation file by downloading it from the Kaspersky website.

To install Kaspersky Security Center Linux:

1. In the command line, run the commands provided in this instruction under an account with root privileges.
2. Create a group 'kladmins' and an unprivileged account 'ksc'. The account must be a member of the 'kladmins' group. To do this, sequentially run the following commands:

```
# adduser ksc  
# groupadd kladmins  
# gpasswd -a ksc kladmins  
# usermod -g kladmins ksc
```
3. Run the Kaspersky Security Center Linux installation. Depending on your Linux distribution, run one of the following commands:

- # apt install /<path>/ksc64_[version_number]_amd64.deb

- # yum install /<path>/ksc64-[version_number].x86_64.rpm -y

4. Run the Kaspersky Security Center Linux configuration:

```
# /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

5. Read the [End User License Agreement](#) (EULA) and the Privacy Policy. The text is displayed in the command line window. Press the space bar to view the next text segment. Then, when prompted, enter the following values:

- a. Enter `y` if you understand and accept the terms of the EULA. Enter `n` if you do not accept the terms of the EULA. To use Kaspersky Security Center Linux, you must accept the terms of the EULA.
- b. Enter `y` if you understand and accept the terms of the Privacy Policy, and you agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. Enter `n` if you do not accept the terms of the Privacy Policy. To use Kaspersky Security Center Linux, you must accept the terms of the Privacy Policy.

6. When prompted, enter the following settings:

- a. Enter the Administration Server DNS name or static IP address. `127.0.0.1` for a local DB installation.

- b. Enter the Administration Server SSL port number. By default, port 13000 is used.

- c. Evaluate the approximate number of devices that you intend to manage:

- If you have from 1 to 100 networked devices, enter 1.
- If you have from 101 to 1000 networked devices, enter 2.
- If you have more than 1000 networked devices, enter 3.

- d. Enter the security group name for services. By default, the `k1admins` group is used.

- e. Enter the account name to start the Administration Server service. The account must be a member of the entered security group. By default, the `ksc` account is used.

- f. Enter the account name to start other services. The account must be a member of the entered security group. By default, the `ksc` account is used.

- g. Select the DBMS that you installed to work with Kaspersky Security Center Linux:

- If you installed MySQL or MariaDB, enter 1.
- If you installed PostgreSQL or Postgres Pro, enter 2.

- h. Enter the DNS name or IP address of the device on which the database is installed. `127.0.0.1` for a local DB installation.

- i. Enter the database port number. This port is used to communicate with Administration Server. By default, the following ports are used:

- Port 3306 for MySQL or MariaDB
- Port 5432 for PostgreSQL or Postgres Pro

- j. Enter the database name.

k. Enter the login of the database root account that you use to access the database.

l. Enter the password of the database root account that you use to access the database.

Wait for the services to be added and started automatically:

- `klagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. Create an account that will act as an Administration Server administrator. Enter the user name and password. You can use the following command to create a new user:

```
/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
```

The password must comply with the following rules:

- The user password cannot have less than 8 or more than 16 characters.
- The password must contain characters from at least three of the groups listed below:
 - Uppercase letters (A-Z)
 - Lowercase letters (a-z)
 - Numbers (0-9)
 - Special characters (@ # \$ % ^ & * - _ ! + = [] { } | : ' . ? / \ ` ~ " () ;)

The user is added and Kaspersky Security Center Linux is installed.

Service verification

Use the following commands to check whether or not a service is running:

- `# systemctl status klagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Installing Kaspersky Security Center Linux in silent mode

You can install Kaspersky Security Center Linux on Linux devices by using an answer file to run an installation in silent mode, that is, without user participation. The answer file contains a custom set of installation parameters: variables and their respective values.

Before installation:

- Install a [database management system \(DBMS\)](#).
- Make sure that the device on which you want to install Kaspersky Security Center Linux is running one of the [supported Linux distributions](#).

To install Kaspersky Security Center Linux in silent mode:

1. Read the [End User License Agreement](#). Follow the steps below only if you understand and accept the terms of the End User License Agreement.
2. Create a group 'kladmins' and an unprivileged account 'ksc', that must be a member of the 'kladmins' group. To do this, sequentially run the following commands under an account with root privileges:


```
# adduser ksc
# groupadd kladmins
# gpasswd -a ksc kladmins
# usermod -g kladmins ksc
```
3. Create the answer file (in TXT format), and add a list of variables in the `VARIABLE_NAME=variable_value` format to the answer file, each one in a separate line. The answer file should include the variables listed in the table below.
4. Set the value of the `KLAUTOANSWERS` environment variable in the root environment containing the full name of the answer file including the path, for example, with the following command:


```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```
5. Run the Kaspersky Security Center Linux installation in silent mode—depending on your Linux distribution, run one of the following commands:
 - `# apt install /<path>/ksc64-[version_number]_amd64.deb`
 - `# yum install /<path>/ksc64-[version_number].x86_64.rpm -y`
6. Create a user to work with Kaspersky Security Center Web Console. To do this, run the following command under an account with root privileges:


```
/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password >
```

, where the password must contain at least 8 characters.

Variables of the answer file used as parameters of Kaspersky Security Center Linux installation in silent mode

| Variable name | Required | Description | Possible values |
|---------------------------|----------|--|-----------------|
| EULA_ACCEPTED | Yes | Confirms that you understand and accept the terms of the End User License Agreement. | 1 |
| PP_ACCEPTED | Yes | Confirms that you understand and accept the terms of the Privacy Policy. | 1 |
| KLSRV_UNATT_SERVERADDRESS | Yes | The Administration Server DNS-name or static IP address. | DNS name or IP |
| KLSRV_UNATT_PORT_SRV | No | The Administration Server port number. Optional, default value is 14000. | Port number |
| KLSRV_UNATT_PORT_SRV_SSL | No | The Administration Server SSL port number. Optional, default value is 13000. | Port number |

| | | | |
|---------------------------|-----|--|--|
| KLSRV_UNATT_PORT_KLOAPI | No | The Administration Server KLOAPI port number. Optional, default value is 13299. | Port number |
| KLSRV_UNATT_PORT_GUI | No | The Administration Server GUI port number. Optional, default value is 13291. | Port number |
| KLSRV_UNATT_NETRANGETYPE | No | The approximate number of devices that you intend to manage. Optional, default value is 1. | 1 for 1 to 100 r devices. 2 for 101 to 1,00 networked dev 3 for more tha networked dev |
| KLSRV_UNATT_DBMS_TYPE | Yes | The database management system type: MySQL (MariaDB) or Postgres. | mysql or postgres |
| KLSRV_UNATT_DBMS_INSTANCE | Yes | The database server IP address. | IP address |
| KLSRV_UNATT_DBMS_PORT | Yes | The database server port. Default value for MySQL (MariaDB) is 3306; default value for Postgres is 5432. | 3306 or 5432 |
| KLSRV_UNATT_DB_NAME | Yes | The database name. | kav |
| KLSRV_UNATT_DBMS_LOGIN | Yes | The username of a user that has access to the database. | |
| KLSRV_UNATT_DBMS_PASSWORD | Yes | The password of a user that has access to the database. | |
| KLSRV_UNATT_KLADMINSGROUP | Yes | The security group name for services. | kladmins |
| KLSRV_UNATT_KLSRVUSER | Yes | The account name to start the Administration Server service. The account must be a member of the security group specified in KLSRV_UNATT_KLADMINSGROUP variable. | ksc |
| KLSRV_UNATT_KLSVCUSER | Yes | The account name to start other services. The account must be a member of the security group specified in KLSRV_UNATT_KLADMINSGROUP variable. | ksc |

If the Administration Server is to be deployed as a [Kaspersky Security Center Linux failover cluster](#), the answers include the following additional variables:

| | | | |
|------------------------------------|-----|---|--------------|
| KLFOC_UNATT_NODE | Yes | The node number (1 or 2). | 1 or 2 |
| KLFOC_UNATT_STATE_SHARE_MOUNT_PATH | Yes | The state share mount point. | |
| KLFOC_UNATT_DATA_SHARE_MOUNT_PATH | Yes | The data share mount point. | |
| KLFOC_UNATT_CONN_MODE | Yes | The failover cluster connectivity mode. | VirtualAdap |

| | | | |
|---|------------------------------------|---|--------------|
| | | | or |
| | | | ExternalLoad |
| In case the KLFOC_UNATT_CONN_MODE variable has VirtualAdapter value, the answer file must include the following additional variables: | | | |
| KLFOC_UNATT_CONN_MODE_VA_NAME | | The virtual network adapter name. | |
| KLFOC_UNATT_CONN_MODE_VA_IPV4 | One of these variables is required | The virtual network adapter IP address. | IP address |
| KLFOC_UNATT_CONN_MODE_VA_IPV6 | | The virtual network adapter IPv6 address. | IPv6 address |

Installing Kaspersky Security Center Linux on Astra Linux in the closed software environment mode

This section describes how to install Kaspersky Security Center Linux on the Astra Linux Special Edition operating system.

Before installation:

- [Install the DBMS.](#)
- Make sure that the device on which you want to install Kaspersky Security Center Linux is running one of the [supported Linux distributions](#).
- Download the [kaspersky_astra_pub_key.gpg application key](#).

Use the ksc64_[version_number]_amd64.deb installation file. You receive the installation file by downloading it from the Kaspersky website.

Run the commands provided in this instruction under an account with root privileges.

To install Kaspersky Security Center Linux on the Astra Linux Special Edition (operational update 1.7.2) and Astra Linux Special Edition (operational update 1.6) operating system:

1. Open the /etc/digsig/digsig_initramfs.conf file, and then specify the following setting:

```
DIGSIG_ELF_MODE=1
```

2. In the command line, run the following command to install the compatibility package:

```
apt install astra-digsig-oldkeys
```

3. Create a directory for the application key:

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

4. Place the application key in the directory created in the previous step:

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

5. Update the RAM disks:

```
update-initramfs -u -k all
```

Reboot the system.

6. Create a group 'kladmins' and an unprivileged account 'ksc'. The account must be a member of the 'kladmins' group. To do this, sequentially run the following commands:

```
# adduser ksc
# groupadd kladmins
# gpasswd -a ksc kladmins
# usermod -g kladmins ksc
```

7. Run the Kaspersky Security Center Linux installation:

```
# apt install /<path>/ksc64_[ version_number ]_amd64.deb
```

8. Run the Kaspersky Security Center Linux configuration:

```
# /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

9. Read the [End User License Agreement](#) (EULA) and the Privacy Policy. The text is displayed in the command line window. Press the space bar to view the next text segment. When prompted, enter the following values:

a. Enter *y* if you understand and accept the terms of the EULA. Enter *n* if you do not accept the terms of the EULA. To use Kaspersky Security Center Linux, you must accept the terms of the EULA.

b. Enter *y* if you understand and accept the terms of the Privacy Policy, and you agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. Enter *n* if you do not accept the terms of the Privacy Policy. To use Kaspersky Security Center Linux, you must accept the terms of the Privacy Policy.

10. When prompted, enter the following settings:

a. Enter the Administration Server DNS name or static IP address.

b. Enter the Administration Server port number. By default, port 14000 is used.

c. Enter the Administration Server SSL port number. By default, port 13000 is used.

d. Evaluate the approximate number of devices that you intend to manage:

- If you have from 1 to 100 networked devices, enter 1.
- If you have from 101 to 1000 networked devices, enter 2.
- If you have more than 1000 networked devices, enter 3.

e. Enter the security group name for services. By default, the 'kladmins' group is used.

f. Enter the account name to start the Administration Server service. The account must be a member of the entered security group. By default, the 'ksc' account is used.

g. Enter the account name to start other services. The account must be a member of the entered security group. By default, the 'ksc' account is used.

h. Enter the IP address of the device on which the database is installed.

i. Enter the database port number. This port is used to communicate with Administration Server. By default, port 3306 is used.

j. Enter the database name.

k. Enter the login of the database root account that you use to access the database.

l. Enter the password of the database root account that you use to access the database.

Wait for the services to be added and started automatically:

- `klagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. Create an account that will act as an Administration Server administrator. Enter the user name and password.

The password must comply with the following rules:

- The user password must have a minimum of 8, and a maximum of 16, characters.
- The password must contain characters from at least three of the groups listed below:
 - Uppercase letters (A-Z)
 - Lowercase letters (a-z)
 - Numbers (0-9)
 - Special characters (@ # \$ % ^ & * - _ ! + = [] { } | : ' . , ? / \ ` ~ " () ;)

Kaspersky Security Center Linux is installed and the user is added.

Service verification

Use the following commands to check whether or not a service is running:

- `# systemctl status klagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Installing Kaspersky Security Center Web Console

This section describes how to install Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) on devices running the Linux operating system. Before installation, you must [install a DBMS](#) and the [Kaspersky Security Center Linux](#) Administration Server.

If you install Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode, follow the [instructions specific for Astra Linux](#).

Use one of the following installation files that corresponds to the Linux distribution installed on your device:

- For Debian—ksc-web-console-[build_number].x86_64.deb
- For RPM-based operating systems—ksc-web-console-[build_number].x86_64.rpm
- For ALT 8 SP—ksc-web-console-[build_number]-alt8p.x86_64.rpm

You receive the installation file by downloading it from the Kaspersky website.

To install Kaspersky Security Center Web Console:

1. Make sure that the device on which you want to install Kaspersky Security Center Web Console is running one of the supported Linux distributions.
2. Read the End User License Agreement (EULA). If the Kaspersky Security Center Linux distribution kit does not include a TXT file with the text of EULA, you can download the file from the [Kaspersky website](#). If you do not accept the terms of the License Agreement, do not install the application.
3. Create a [response file](#) that contains parameters for connecting Kaspersky Security Center Web Console to the Administration Server. Name this file ksc-web-console-setup.json and place it in the following directory: /etc/ksc-web-console-setup.json.

Example of a response file containing the minimal set of parameters and the default address and port:

```
{
  "address": "127.0.0.1",
  "port": 8080,
  "trusted":
  "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/k1server.cer|KSC
  Server",
  "acceptEula": true
}
```

When you install Kaspersky Security Center Web Console on Linux ALT operating system, you must specify a port number other than 8080, because port 8080 is used by the operating system.

Kaspersky Security Center Web Console cannot be updated by using the same .rpm installation file. If you want to change settings in a response file and use this file to reinstall the application, you must first remove the application, and then install it again with the new response file.

4. Under an account with root privileges, use the command line to run the setup file with the .deb or .rpm extension, depending on your Linux distribution.
 - To install or upgrade Kaspersky Security Center Web Console from a .deb file, run the following command:
\$ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
 - To install Kaspersky Security Center Web Console from an .rpm file, run one of the following commands:
\$ sudo rpm -ivh --nodeps ksc-web-console-[build_number].x86_64.rpmor

```
$ sudo alien -i ksc-web-console-[ build_number ].x86_64.rpm
```

- To upgrade from a previous version of Kaspersky Security Center Web Console, run one of the following commands:
 - For devices running RPM-based operating system:

```
$ sudo rpm -Uvh --nodeps --force ksc-web-console-[ build_number ].x86_64.rpm
```
 - For devices running Debian-based operating system:

```
$ sudo dpkg -i ksc-web-console-[ build_number ].x86_64.deb
```

This starts unpacking of the setup file. Please wait until the installation is complete. Kaspersky Security Center Web Console is installed to the following directory: `/var/opt/kaspersky/ksc-web-console`.

5. Restart all of the Kaspersky Security Center Web Console services by running the following command:
- ```
$ sudo systemctl restart KSC*
```

When the installation is complete, you can use your browser to [open and log in to Kaspersky Security Center Web Console](#).

## Kaspersky Security Center Web Console installation parameters

For [installing Kaspersky Security Center Web Console Server on devices running Linux](#), you must create a response file—a .json file that contains parameters for connecting Kaspersky Security Center Web Console to the Administration Server.

Here is an example of a response file containing the minimal set of parameters and the default address and port:

```
{
 "address": "127.0.0.1",
 "port": 8080,
 "defaultLangId": 1049,
 "enableLog": false,
 "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
 "acceptEula": true,
 "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
 "webConsoleAccount": "Group1 : User1",
 "managementServiceAccount": "Group1 : User2",
 "serviceWebConsoleAccount": "Group1 : User3",
 "pluginAccount": "Group1 : User4",
 "messageQueueAccount": "Group1 : User5"
}
```

When you install Kaspersky Security Center Web Console on the Linux ALT operating system, you must specify a port number other than 8080, because port 8080 is used by the operating system.

The table below describes the parameters that can be specified in a response file.

Parameters for installing Kaspersky Security Center Web Console on devices running Linux

| Parameter | Description                   | Available value |
|-----------|-------------------------------|-----------------|
| address   | Address of Kaspersky Security | String value.   |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | Center Web Console Server (required).                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| port          | Number of port that Kaspersky Security Center Web Console Server uses to connect to the Administration Server (required).                                                                                                                                                                                                                                                                                        | Numerical value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| defaultLangId | Language of user interface (by default, 1033).                                                                                                                                                                                                                                                                                                                                                                   | <p>Numerical code of the language:</p> <ul style="list-style-type: none"> <li>• German: 1031</li> <li>• English: 1033</li> <li>• Spanish: 3082</li> <li>• Spanish (Mexico): 2058</li> <li>• French: 1036</li> <li>• Japanese: 1041</li> <li>• Kazakh: 1087</li> <li>• Polish: 1045</li> <li>• Portuguese (Brazil): 1046</li> <li>• Russian: 1049</li> <li>• Turkish: 1055</li> <li>• Simplified Chinese: 4</li> <li>• Traditional Chinese: 31748</li> </ul> <p>If no value is specified, then English (en-U</p> |
| enableLog     | Whether or not to enable Kaspersky Security Center Web Console activity logging.                                                                                                                                                                                                                                                                                                                                 | <p>Boolean value:</p> <ul style="list-style-type: none"> <li>• true—Logging is enabled (selected by</li> <li>• false—Logging is disabled.</li> </ul>                                                                                                                                                                                                                                                                                                                                                            |
| trusted       | <p>List of trusted Administration Servers allowed to connect to Kaspersky Security Center Web Console. Each Administration Server must be defined with the following parameters:</p> <ul style="list-style-type: none"> <li>• Administration Server address</li> <li>• OpenAPI port that is used by Kaspersky Security Center Web Console to connect to the Administration Server (by default, 13299)</li> </ul> | <p>String value in the following format:</p> <p>" server address   port   certificat</p> <p>Example:</p> <p>"X.X.X.X 13299 /cert/server-1.cer<br/>1   Y.Y.Y.Y 13299 /cert/server-2.</p>                                                                                                                                                                                                                                                                                                                         |

|                          |                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <ul style="list-style-type: none"> <li>• Path to the certificate of the Administration Server</li> <li>• Administration Server name that will be displayed in the login window</li> </ul> <p>The parameters are separated with vertical bars. If several Administration Servers are specified, separate them with two vertical bars (pipes).</p> |                                                                                                                                                                                                                                                                                                                                                                |
| acceptEula               | <p>Whether or not you want to accept the terms of the <a href="#">End User License Agreement</a> (EULA). The file containing the terms of the EULA is downloaded together with the installation file.</p>                                                                                                                                        | <p>Boolean value:</p> <ul style="list-style-type: none"> <li>• true—I have fully read, understand, and <a href="#">End User License Agreement</a>.</li> <li>• false—I do not accept the terms of t (selected by default).</li> </ul> <p>If no value is specified, the Kaspersky Sec installer shows you the EULA and asks wh accept the terms of the EULA.</p> |
| certDomain               | <p>If you want to generate a new certificate, use this parameter to specify the domain name for which a new certificate is to be generated.</p>                                                                                                                                                                                                  | <p>String value.</p>                                                                                                                                                                                                                                                                                                                                           |
| certPath                 | <p>If you want to use an existing certificate, use this parameter to specify the path to the certificate file.</p>                                                                                                                                                                                                                               | <p>String value.</p> <p>Specify the path <code>"/var/opt/kaspersky/klnagent_srv/</code> to use the existing certificate. For a custc path where this custom certificate is stor</p>                                                                                                                                                                            |
| keyPath                  | <p>If you want to use an existing certificate, use this parameter to specify path to the key file.</p>                                                                                                                                                                                                                                           | <p>String value.</p>                                                                                                                                                                                                                                                                                                                                           |
| webConsoleAccount        | <p>Name of the account under which the <a href="#">KSCWebConsole</a> service is run.</p>                                                                                                                                                                                                                                                         | <p>String value in the following format: " gro</p> <p>Example: " Group1 : User1 " .</p> <p>If no value is specified, the Kaspersky Sec installer creates a new account with the c user_management_%uid%.</p>                                                                                                                                                   |
| managementServiceAccount | <p>Name of the privileged account under which the <a href="#">KSCWebConsoleManagement</a> service is run.</p>                                                                                                                                                                                                                                    | <p>String value in the following format: " gro</p> <p>Example: " Group1 : User1 " .</p> <p>If no value is specified, the Kaspersky Sec installer creates a new account with the c user_nodejs_%uid%.</p>                                                                                                                                                       |
| serviceWebConsoleAccount | <p>Name of the account under which the <a href="#">KSCSvcWebConsole</a> service is run.</p>                                                                                                                                                                                                                                                      | <p>String value in the following format: " gro</p> <p>Example: " Group1 : User1 " .</p> <p>If no value is specified, the Kaspersky Sec installer creates a new account with the c user_svc_nodejs_%uid%.</p>                                                                                                                                                   |
|                          |                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                |

|                     |                                                                                               |                                                                                                                                                                                                             |
|---------------------|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pluginAccount       | Name of the account under which the <a href="#">KSCWebConsolePlugin</a> service is run.       | String value in the following format: " group : user ".<br>Example: " Group1 : User1 ".<br>If no value is specified, the Kaspersky Sec installer creates a new account with the c user_web_plugin_%uid%.    |
| messageQueueAccount | Name of the account under which the <a href="#">KSCWebConsoleMessageQueue</a> service is run. | String value in the following format: " group : user ".<br>Example: " Group1 : User1 ".<br>If no value is specified, the Kaspersky Sec installer creates a new account with the c user_message_queue_%uid%. |

If you specify the `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, or `messageQueueAccount` parameters, make sure that the custom user accounts belong to the same security group. If these parameters are not specified, the Kaspersky Security Center Web Console installer creates a default security group, and then creates user accounts with default names in this group.

## Installing Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode

This section describes how to install Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) on the Astra Linux Special Edition operating system. Before installation, you must [install a DBMS](#) and the [Kaspersky Security Center Linux](#) Administration Server.

*To install Kaspersky Security Center Web Console:*

1. Make sure that the device on which you want to install Kaspersky Security Center Web Console is running one of the supported Linux distributions.
2. Read the End User License Agreement (EULA). If the Kaspersky Security Center Linux distribution kit does not include a TXT file with the text of EULA, you can download the file from the [Kaspersky website](#). If you do not accept the terms of the License Agreement, do not install the application.
3. Create a [response file](#) that contains parameters for connecting Kaspersky Security Center Web Console to the Administration Server. Name this file `ksc-web-console-setup.json` and place it in the following directory: `/etc/ksc-web-console-setup.json`.

Example of a response file containing the minimal set of parameters and the default address and port:

```
{
 "address": "127.0.0.1",
 "port": 8080,
 "trusted":
 "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
 Server",
 "acceptEula": true
}
```

4. Open the `/etc/digsig/digsig_initramfs.conf` file, and then specify the following setting:

```
DIGSIG_ELF_MODE=1
```

5. In the command line, run the following command to install the compatibility package:

```
apt install astra-digsig-oldkeys
```

6. Create a directory for the application key:

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

7. Place the application key `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` in the directory created in the previous step:

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

If the Kaspersky Security Center Linux distribution kit does not include the `kaspersky_astra_pub_key.gpg` application key, you can download it by clicking the link:

[https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky\\_astra\\_pub\\_key.gpg](https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg).

8. Update the RAM disks:

```
update-initramfs -u -k all
```

Reboot the system.

9. Under an account with root privileges, use the command line to run the setup file. You receive the setup file by downloading it from the Kaspersky website.

- To install or upgrade Kaspersky Security Center Web Console, run the following command:  
\$ sudo dpkg -i ksc-web-console-[build\_number].x86\_64.deb
- To upgrade from a previous version of Kaspersky Security Center Web Console, run the following command:  
\$ sudo dpkg -i ksc-web-console-[build\_number].x86\_64.deb

This starts unpacking of the setup file. Please wait until the installation is complete. Kaspersky Security Center Web Console is installed to the following directory: `/var/opt/kaspersky/ksc-web-console`.

10. Restart all of the Kaspersky Security Center Web Console services by running the following command:

```
$ sudo systemctl restart KSC*
```

When the installation is complete, you can use your browser to [open and log in to Kaspersky Security Center Web Console](#).

## Installing Kaspersky Security Center Web Console connected to Administration Server installed on Kaspersky Security Center Linux failover cluster nodes

This section describes how to install Kaspersky Security Center Web Console Server (hereinafter also referred to as Kaspersky Security Center Web Console), that connects to Administration Server installed on Kaspersky Security Center Linux failover cluster nodes. Prior to installing Kaspersky Security Center Web Console, [install a DBMS](#) and Kaspersky Security Center Linux Administration Server on [Kaspersky Security Center Linux failover cluster nodes](#).

*To install Kaspersky Security Center Web Console that connects to Administration Server installed on Kaspersky Security Center Linux failover cluster nodes:*

1. Perform step 1 and step 2 of the [Kaspersky Security Center Web Console installation](#).

2. At step 3, in the [response file](#), specify the trusted installation parameter to allow the Kaspersky Security Center Linux failover cluster to connect to Kaspersky Security Center Web Console. The string value of this parameter has the following format:

```
"trusted": "server address|port|certificate path|server name"
```

Specify the components of the trusted installation parameter:

- **Administration Server address.** If you created a secondary network adapter when [preparing the cluster nodes](#), use the IP address of the adapter as the Kaspersky Security Center Linux failover cluster address. Otherwise, specify the IP address of the third-party load balancer that you use.
- **Administration Server port.** The OpenAPI port that Kaspersky Security Center Web Console uses to connect to Administration Server (default value is 13299).
- **Administration Server certificate.** The Administration Server certificate is located in the shared data storage of the [Kaspersky Security Center Linux failover cluster](#). The default path to the certificate file is: <shared data folder>\1093\cert\klserver.cer. Copy the certificate file from the shared data storage to the device where you install Kaspersky Security Center Web Console. Specify the local path to the Administration Server certificate.
- **Administration Server name.** The Kaspersky Security Center Linux failover cluster name that will be displayed in the login window of Kaspersky Security Center Web Console.

3. Continue with the standard installation of Kaspersky Security Center Web Console.

After the installation is complete, a shortcut appears on your desktop, and you can [log in](#) to Kaspersky Security Center Web Console.

You can go to **Discovery & deployment** → **Unassigned devices** to view the information about the cluster nodes and the [file server](#).

## Deployment of the Kaspersky Security Center Linux failover cluster

This section contains both general information about the Kaspersky Security Center Linux failover cluster, and instructions on the preparation and deployment of the Kaspersky Security Center Linux failover cluster in your network.

### Scenario: Deployment of Kaspersky Security Center Linux failover cluster

A Kaspersky Security Center Linux failover cluster provides high availability of Kaspersky Security Center Linux and minimizes downtime of Administration Server in case of a failure. The failover cluster is based on two identical instances of Kaspersky Security Center Linux installed on two computers. One of the instances works as an active node and the other one is a passive node. The active node manages protection of the client devices, while the passive one is prepared to take all of the functions of the active node in case the active node fails. When a failure occurs, the passive node becomes active and the active node becomes passive.

#### Prerequisites

You have the hardware that meets the [requirements](#) for the failover cluster.

Kaspersky applications deployment proceeds in stages:

## 1 Creating accounts for Kaspersky Security Center Linux services

Perform the following steps on the active node, passive node, and the file server:

1. Create a domain group with the name 'kladmins' and assign the same GID to all three groups.
2. Create a user account with the name 'ksc' and assign the same UID to all three user accounts. Set the primary group to 'kladmins' for the created accounts.
3. Create a user account with the name 'rightless' and assign the same UID to all three user accounts. Set the primary group to 'kladmins' for the created accounts.

## 2 File server preparation

Prepare the file server to work as a component of Kaspersky Security Center Linux failover cluster. Make sure that the file server meets the hardware and software requirements, create two shared folders for Kaspersky Security Center Linux data, and configure permissions to access the shared folders.

How-to instructions: [Preparing a file server for Kaspersky Security Center Linux failover cluster](#)

## 3 Preparation of active and passive nodes

Prepare two computers with identical hardware and software to work as an active and passive nodes.

How-to instructions: [Preparing nodes for Kaspersky Security Center Linux failover cluster](#)

## 4 Database Management System (DBMS) installation

You have two options:

- o If you want to use MariaDB Galera Cluster, you do not need a dedicated computer for DBMS. Install MariaDB Galera Cluster on each of the nodes.
- o If you want to use any other [supported DBMS](#), [install](#) the selected DBMS on a dedicated computer.

## 5 Kaspersky Security Center Linux installation

Install Kaspersky Security Center Linux in the failover cluster mode on both nodes. You must first install Kaspersky Security Center Linux on the active node, and then install it on the passive one.

Additionally, you can [install Kaspersky Security Center Web Console](#) on a separate device that is not a cluster node.

## 6 Testing the failover cluster

Check that you configured the failover cluster correctly and it works properly. For example, you can stop one of the Kaspersky Security Center Linux services on the active node: kladminserver, klnagent, ksnproxy, klactprx, or klwebsrv. After the service stopped, the protection management must be automatically switched to the passive node.

## Results

Kaspersky Security Center Linux failover cluster is deployed. Please be acquainted with the [events that lead to the switch between the active and passive nodes](#).

## About Kaspersky Security Center Linux failover cluster



A Kaspersky Security Center Linux failover cluster provides high availability of Kaspersky Security Center Linux and minimizes downtime of Administration Server in case of a failure. The failover cluster is based on two identical instances of Kaspersky Security Center Linux installed on two computers. One of the instances works as an active node and the other one is a passive node. The active node manages protection of the client devices, while the passive one is prepared to take all of the functions of the active node in case the active node fails. When a failure occurs, the passive node becomes active and the active node becomes passive.

In a Kaspersky Security Center Linux failover cluster, all Kaspersky Security Center Linux services are managed automatically. Do not try to restart the services manually.

## Hardware and software requirements

To deploy a Kaspersky Security Center Linux failover cluster, you must have the following hardware:

- Two computers with identical hardware and software. These computers will act as the active and passive nodes.
- A file server running Linux, with the EXT4 file system. You must provide a dedicated computer that will act as a file server.

Make sure you have provided high network bandwidth between the file server, and the active and passive nodes.

- A computer with Database Management System (DBMS). If you use MariaDB Galera Cluster as a DBMS, a dedicated computer for this purpose is not required.

## Switch conditions

The failover cluster switches protection management of the client devices from the active node to the passive one, if any of the following events occurs on the active node:

- The active node is broken due to a software or hardware failure.
- The active node was temporarily stopped for [maintenance](#) activities.
- At least one of the Kaspersky Security Center Linux services (or processes) failed or was deliberately terminated by user. The Kaspersky Security Center Linux services are the following ones: kladminserver, klnagent, klactprx, and klwebsrv.
- The network connection between the active node and the storage on the file server was interrupted or terminated.

## Preparing a file server for a Kaspersky Security Center Linux failover cluster

A file server works as a required component of a [Kaspersky Security Center Linux failover cluster](#).

*To prepare a file server:*

1. Make sure that the file server meets the [hardware and software requirements](#).

2. Install and configure an NFS server:

- Access to the file server must be enabled for both nodes in the NFS server settings.
- The NFS protocol must have version 4.0 or 4.1.
- Minimum requirements for Linux kernel:
  - 3.19.0-25, if you use NFS 4.0
  - 4.4.0-176, if you use NFS 4.1

3. On the file server, create two folders and share them by using NFS. One of them is used to keep information about the failover cluster state. The other one is used to store the data and settings of Kaspersky Security Center Linux. You will specify paths to the shared folders while configuring the [installation of Kaspersky Security Center Linux](#).

Run the following commands:

```
sudo yum install nfs-utils
sudo mkdir -p /mnt/KlFocStateShare
sudo mkdir -p /mnt/KlFocDataShare_klfoc
sudo chown ksc:kladmins /mnt/KlFocStateShare
sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
sudo sh -c "echo /mnt/KlFocStateShare *(rw, sync, no_subtree_check, no_root_squash) >> /etc/exports"
sudo sh -c "echo /mnt/KlFocDataShare_klfoc *(rw, sync, no_subtree_check, no_root_squash) >> /etc/exports"
sudo cat /etc/exports
sudo exportfs -a
sudo systemctl start rpcbind
sudo service nfs start
```

Enable autostart by running the following command:

```
sudo systemctl enable rpcbind
```

4. Restart the file server.

The file server is prepared. To deploy the Kaspersky Security Center Linux failover cluster, follow the further instructions in this [scenario](#).

## Preparing nodes for a Kaspersky Security Center Linux failover cluster

Prepare two computers to work as the active and passive nodes of the [Kaspersky Security Center Linux failover cluster](#).

*To prepare nodes for the Kaspersky Security Center Linux failover cluster:*

1. Make sure that you have two computers that meet the [hardware and software requirements](#). These computers will act as the active and passive nodes of the failover cluster.
2. To make the nodes function as NFS clients, install the nfs-utils package on each node.

Run the following command:

```
sudo yum install nfs-utils
```

3. Create mount points by running the following commands:

```
sudo mkdir -p /mnt/KlFocStateShare
sudo mkdir -p /mnt/KlFocDataShare_klfoc
```

4. Check that the shared folders can be successfully mounted. [optional step]

Run the following commands:

```
sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {server}:{path to
the KlFocStateShare folder} /mnt/KlFocStateShare
sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {server}:{path to
the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc
```

Here, {server}:{path to the KlFocStateShare folder} and {server}:{path to the KlFocDataShare\_klfoc folder} are the network paths to the shared folders on the file server.

After the shared folders have been successfully mounted, unmount them by running the following commands:

```
sudo umount /mnt/KlFocStateShare
sudo umount /mnt/KlFocDataShare_klfoc
```

5. Match the mount points and the shared folders:

```
sudo vi /etc/fstab
{server}:{path to the KlFocStateShare folder} /mnt/KlFocStateShare nfs
vers=4,nolock,local_lock=none,auto,user,rw 0 0
{server}:{path to the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc nfs
vers=4,nolock,local_lock=none,noauto,user,rw 0 0
```

Here, {server}:{path to the KlFocStateShare folder} and {server}:{path to the KlFocDataShare\_klfoc folder} are the network paths to the shared folders on the file server.

6. Restart both nodes.

7. Mount the shared folders by running the following commands:

```
mount /mnt/KlFocStateShare
mount /mnt/KlFocDataShare_klfoc
```

8. Ensure that the permissions to access the shared folders belong to ksc:kladmins.

Run the following command:

```
sudo ls -la /mnt/
```

9. On each of the nodes, configure a secondary network adapter.

A secondary network adapter can be physical or virtual. If you want to use a physical network adapter, connect and configure it with standard operating system tools. If you want to use a virtual network adapter, create it by using third-party software.

Do one of the following:

- Use a virtual network adapter.
  - a. Use the following command to check that NetworkManager is used to manage the physical adapter:

```
nmcli device status
```

If the physical adapter is shown as unmanaged in the output, configure NetworkManager to manage the physical adapter. The exact configuration steps depend on your distribution.

- b. Use the following command to identify interfaces:

```
ip a
```

- c. Create a new configuration profile:

```
nmcli connection add type macvlan dev <physical interface> mode bridge
ifname <virtual interface> ipv4.addresses <address mask> ipv4.method manual
autoconnect no
```

- Use a physical network adapter or a hypervisor. In this scenario, disable the software NetworkManager.

- a. Delete NetworkManager connections for the target interface:

```
nmcli con del <connection name>
```

Use the following command to check if the target interface has connections:

```
nmcli con show
```

- b. Edit the NetworkManager.conf file. Locate the keyfile section and assign the target interface to the unmanaged-devices parameter.

```
[keyfile]
unmanaged-devices=interface-name:<interface name>
```

- c. Restart NetworkManager:

```
systemctl reload NetworkManager
```

Use the following command to verify that the target interface is unmanaged:

```
nmcli dev status
```

- Use a third-party load balancer. For example, you can use an nginx server. In this case, do the following:
  - a. Provide a dedicated Linux-based computer with nginx installed.
  - b. Configure load balancing. Set the active node as the main server, and the passive node as a backup server.
  - c. On the nginx server, open all of the Administration Server ports: TCP 13000, UDP 13000, TCP 13291, TCP 13299, TCP 17000.

The nodes are prepared. To deploy Kaspersky Security Center Linux failover cluster, follow the further instructions of the [scenario](#).

## Installing Kaspersky Security Center Linux on the Kaspersky Security Center Linux failover cluster nodes

This procedure describes how to install Kaspersky Security Center Linux on the nodes of the [Kaspersky Security Center Linux failover cluster](#). Kaspersky Security Center Linux is installed on both nodes of the Kaspersky Security Center Linux failover cluster separately. First, you install the application on the active node, then on the passive one. When installing, you choose which node will be active and which will be passive.

Use the installation file—ksc64-[version\_number]-amd64.deb or ksc64-[version\_number].x86\_64.rpm—that corresponds to the Linux distribution installed on your device. You receive the installation file by downloading it from the Kaspersky website.

Only a user from the KLAdmins domain group can install Kaspersky Security Center Linux on every node.

## Installation on the primary (active) node

To install Kaspersky Security Center Linux on the primary node:

1. Make sure that the device on which you want to install Kaspersky Security Center Linux is running one of the [supported Linux distributions](#).
2. In the command line, run the commands provided in this instruction under an account with root privileges.
3. Run the Kaspersky Security Center Linux installation. Depending on your Linux distribution, run one of the following commands:
  - `sudo apt install /<path>/ksc64-[ version_number ]_amd64.deb`
  - `sudo yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`
4. Run the Kaspersky Security Center Linux configuration:  
`sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`
5. Read the [End User License Agreement](#) (EULA) and the Privacy Policy. The text is displayed in the command line window. Press the space bar to view the next text segment. Then, when prompted, enter the following values:
  - a. Enter `y` if you understand and accept the terms of the EULA. Enter `n` if you do not accept the terms of the EULA. To use Kaspersky Security Center Linux, you must accept the terms of the EULA.
  - b. Enter `y` if you understand and accept the terms of the Privacy Policy, and you agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. Enter `n` if you do not accept the terms of the Privacy Policy. To use Kaspersky Security Center Linux, you must accept the terms of the Privacy Policy.
6. Select **Primary cluster node** as an Administration Server installation mode.
7. When prompted, enter the following settings:
  - a. Enter the local path to the mount point of the state share.
  - b. Enter the local path to the mount point of the data share.
  - c. Choose a failover cluster connectivity mode: through a secondary network adapter or an external load balancer.
  - d. If you use a secondary network adapter, enter its name.
  - e. When you are prompted to enter the Administration Server DNS name or static IP address, enter the IP address of the secondary network adapter or the IP address of the external load balancer.
  - f. Enter the Administration Server SSL port number. By default, port 13000 is used.
  - g. Evaluate the approximate number of devices that you intend to manage:
    - If you have from 1 to 100 networked devices, enter 1.
    - If you have from 101 to 1000 networked devices, enter 2.
    - If you have more than 1000 networked devices, enter 3.

- h. Enter the security group name for services. By default, the 'kladmins' group is used.
- i. Enter the account name to start the Administration Server service. The account must be a member of the entered security group. By default, the 'ksc' account is used.
- j. Enter the account name to start other services. The account must be a member of the entered security group. By default, the 'ksc' account is used.
- k. Select the DBMS that you installed to work with Kaspersky Security Center Linux:
- If you installed MySQL or MariaDB, enter 1.
  - If you installed PostgreSQL or Postgres Pro, enter 2.
- l. Enter the DNS name or IP address of the device on which the database is installed.
- m. Enter the database port number. This port is used to communicate with Administration Server. By default, the following ports are used:
- Port 3306 for MySQL or MariaDB
  - Port 5432 for PostgreSQL or Postgres Pro
- n. Enter the database name.
- o. Enter the login of the database root account that you use to access the database.
- p. Enter the password of the database root account that you use to access the database.
- Wait for the services to be added and started automatically:
- klnagent\_srv
  - kladminserver\_srv
  - klactprx\_srv
  - klwebsrv\_srv
- q. Create an account that will act as an Administration Server administrator. Enter the user name and password. The user password cannot have less than 8 or more than 16 characters.

The user is added and Kaspersky Security Center Linux is installed on the primary node.

## Installation on the secondary (passive) node

*To install Kaspersky Security Center Linux on the secondary node:*

1. Make sure that the device on which you want to install Kaspersky Security Center Linux is running one of the [supported Linux distributions](#).
2. In the command line, run the commands provided in this instruction under an account with root privileges.
3. Run the Kaspersky Security Center Linux installation. Depending on your Linux distribution, run one of the following commands:

- `sudo apt install /<path>/ksc64-[ version_number ]_amd64.deb`
- `sudo yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`

4. Run the Kaspersky Security Center Linux configuration:

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

5. Read the [End User License Agreement](#) (EULA) and the Privacy Policy. The text is displayed in the command line window. Press the space bar to view the next text segment. Then, when prompted, enter the following values:

- Enter `y` if you understand and accept the terms of the EULA. Enter `n` if you do not accept the terms of the EULA. To use Kaspersky Security Center Linux, you must accept the terms of the EULA.
- Enter `y` if you understand and accept the terms of the Privacy Policy, and you agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. Enter `n` if you do not accept the terms of the Privacy Policy. To use Kaspersky Security Center Linux, you must accept the terms of the Privacy Policy.

6. Select **Secondary cluster node** as an Administration Server installation mode.

7. When prompted, enter the local path to the mount point of the state share.

Kaspersky Security Center Linux is installed on the secondary node.

## Service verification

Use the following commands to check whether or not a service is running:

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

Now, you can test the Kaspersky Security Center Linux failover cluster to make sure that you configured it correctly and that the cluster works properly.

## Starting and stopping cluster nodes manually

You may need to stop the entire Kaspersky Security Center Linux failover cluster or temporarily detach one of the nodes of the cluster for maintenance. If this is the case, follow the instructions in this section. Do not try to start or stop the services or processes related to the failover cluster by using any other means. This may cause data loss.

### Starting and stopping the entire failover cluster for maintenance

*To start or stop the entire failover cluster:*

1. On the active node, go to `/opt/kaspersky/ksc64/sbin`.
2. Open the command line, and then run one of the following commands:

- To stop the cluster, run: `k1foc -stopcluster --stp k1foc`
- To start the cluster, run: `k1foc -startcluster --stp k1foc`

The failover cluster is started or stopped, depending on the command that you run.

## Maintaining one of the nodes

*To maintain one of the nodes:*

1. On the active node, stop the failover cluster by using the `k1foc -stopcluster --stp k1foc` command.
2. On the node that you want to maintain, go to `/opt/kaspersky/ksc64/sbin`.
3. Open command line, and then detach the node from the cluster by running the `detach_node.sh` command.
4. On the active node, start the failover cluster by using the `k1foc -startcluster --stp k1foc` command.
5. Perform maintenance activities.
6. On the active node, stop the failover cluster by using the `k1foc -stopcluster --stp k1foc` command.
7. On the node that was maintained, go to `/opt/kaspersky/ksc64/sbin`.
8. Open command line, and then attach the node to the cluster by running the `attach_node.sh` command.
9. On the active node, start the failover cluster by using the `k1foc -startcluster --stp k1foc` command.

The node is maintained and attached to the failover cluster.

## Accounts for working with the DBMS

To install Administration Server and work with it, you need an internal DBMS account. This account allows you to access the DBMS and requires specific rights. A set of the required rights depends on the following criteria:

- DBMS type:
  - MySQL or MariaDB
  - PostgreSQL or Postgres Pro
- Method of the Administration Server database creation:
  - **Automatic.** During the Administration Server installation, you can automatically create an Administration Server database (hereinafter also referred to as a Server database) by using the Administration Server installer (the installer).
  - **Manual.** You can use a third-party application (for example, SQL Server Management Studio) or a script to create an empty database. After that, you can specify this database as the Server database during the Administration Server installation.



Follow the principle of least privilege when you grant rights and permissions to the accounts. This means that the granted rights should be only enough to perform the required actions.

The tables below contain information about the DBMS rights that you should grant to the accounts before you install and start Administration Server.

## MySQL and MariaDB

If you choose MySQL or MariaDB as a DBMS, create a DBMS internal account to access the DBMS, and then grant this account the required rights. Note that the database creation method does not affect the set of rights. The required rights are listed below:

- Schema privileges:
  - Administration Server database: ALL (excluding GRANT OPTION).
  - System schemes (mysql and sys): SELECT, SHOW VIEW.
  - The sys.table\_exists stored procedure: EXECUTE (if you use MariaDB 10.5 or earlier as a DBMS, you do not need to grant the EXECUTE privilege).
- Global privileges for all schemes: PROCESS, SUPER.

For more information on how to configure the account rights, see [Configuring the DBMS account for work with MySQL and MariaDB](#).

## Configuring privileges for Administration Server data recovery

Rights that you granted to the internal DBMS account are enough to restore Administration Server data from the backup.

## PostgreSQL or Postgres Pro

If you choose PostgreSQL or Postgres Pro as a DBMS, you can use the *postgres* user (the default Postgres role) or create a new Postgres role (hereinafter also referred to as a role) to access the DBMS. Depending on the creation method of the Server database, grant the required rights to the role as described in the table below. For more information on how to configure rights of the role, see [Configuring the DBMS account for work with PostgreSQL or Postgres Pro](#).

Rights of the Postgres role

| Automatic database creation                                  |                                      | Manual database creation                                                                                                                                                                                                                                |
|--------------------------------------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The <i>postgres</i> user does not require additional rights. | Privileges for a new role: CREATEDB. | For a new role: <ul style="list-style-type: none"> <li>• Privileges on Administration Server database: ALL.</li> <li>• Privileges on all tables in the public schema: ALL.</li> <li>• Privileges on all sequences in the public schema: ALL.</li> </ul> |

## Configuring privileges for Administration Server data recovery

To restore Administration Server data from the backup, the Postgres role used to access to the DBMS must have the owner rights on the Administration Server database.

## Configuring the DBMS account for work with MySQL and MariaDB

### Prerequisites

Before you assign rights to the DBMS account, perform the following actions:

1. Make sure that you log in to the system under the local administrator account.
2. Install an environment for working with MySQL or MariaDB.

### Configuring the DBMS account to install Administration Server

*To configure the DBMS account for the Administration Server installation:*

1. Run an environment for working with MySQL or MariaDB under the root account that you created when you installed the DBMS.
2. Create an internal DBMS account with a password. The Administration Server installer (hereinafter also referred to as the installer) and the Administration Server service will use this internal DBMS account to access DBMS.

To create a DBMS account with a password, execute the following command:

```
/* Create a user named KSCAdmin and specify the password for KSCAdmin */
CREATE USER 'KSCAdmin' IDENTIFIED BY '<password>';
```

If you use MySQL 8.0 or earlier as a DBMS, note that for these versions the "Caching SHA2 password" authentication is not supported. Change the default authentication from "Caching SHA2 password" to "MySQL native password":

- To create a DBMS account that uses the "MySQL native password" authentication, execute the following command:  

```
CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
```
- To change the authentication for an existing DBMS account, execute the following command:  

```
ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
```

3. Grant the following privileges to the created DBMS account:

- Schema privileges:
  - Administration Server database: ALL (excluding GRANT OPTION)
  - System schemes (mysql and sys): SELECT, SHOW VIEW
  - The sys.table\_exists stored procedure: EXECUTE
- Global privileges for all schemes: PROCESS, SUPER

To grant the required privileges to the created DBMS account, run the following script:

```
/* Grant privileges to KSCAdmin */
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

If you use MariaDB 10.5 or earlier as a DBMS, you do not need to grant the EXECUTE privilege. In this case, exclude the following command from the script: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

4. To view the list of privileges granted to the DBMS account, execute the following command:

```
SHOW grants for 'KSCAdmin';
```

5. To create an Administration Server database manually, run the following script (in this script, the Administration Server database name is *kav*):

```
CREATE DATABASE kav
DEFAULT CHARACTER SET utf8
DEFAULT COLLATE utf8_general_ci;
```

Use the same database name that you specify in the script that creates the DBMS account.

## 6. [Install Administration Server.](#)

After the installation finishes, the Administration Server database is created and Administration Server is ready to use.

# Configuring the DBMS account for work with PostgreSQL and Postgres Pro

## Prerequisites

Before you assign rights to the DBMS account, perform the following actions:

1. Make sure that you log in to the system under the local administrator account.
2. Install an environment for working with PostgreSQL and Postgres Pro.

## Configuring the DBMS account to install Administration Server (automatic creation of the Administration Server database)

*To configure the DBMS account for the Administration Server installation:*

1. Run an environment for working with PostgreSQL and Postgres Pro.
2. Choose a Postgres role to access the DBMS. You can use one of the following roles:

- The *postgres* user (the default Postgres role).

If you use the *postgres* user, you do not need to grant additional rights to it.

By default, the *postgres* user does not have a password. However, a password is required to install Kaspersky Security Center Linux. To set a password for the *postgres* user, run the following script:

```
ALTER USER user_name WITH PASSWORD '< password >';
```

- A new Postgres role.

If you want to use a new Postgres role, create this role, and then grant it the CREATEDB privilege. To do this, run the following script (in this script, the role is *KCSAdmin*):

```
CREATE USER "KCSAdmin" WITH PASSWORD '< password >' CREATEDB;
```

The created role will be used as an owner of the Administration Server database (hereinafter also referred to as the Server database).

### 3. [Install Administration Server.](#)

After the installation finishes, the Server database is automatically created and Administration Server is ready to use.

## Configuring the DBMS account to install Administration Server (manual creation of the Administration Server database)

*To configure the DBMS account for the Administration Server installation:*

1. Run an environment for working with Postgres.
2. Create a new Postgres role and an Administration Server database. Then, grant all privileges to the role on the Administration Server database. To do this, log in under the *postgres* user in the *postgres* database, and then run the following script (in this script, the role is *KCSAdmin*, the Administration Server database name is *KAV*):

```
CREATE USER "KCSAdmin" WITH PASSWORD '<password>';
CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KCSAdmin";
GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KCSAdmin";
```

If the error "New encoding (UTF8) is incompatible with the encoding of the template database" occurs, create a database by using the command:

```
CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KCSAdmin" TEMPLATE template0;
instead of:
CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KCSAdmin";
```

3. Grant the following privileges to the created Postgres role:

- Privileges on all tables in the public schema: ALL
- Privileges on all sequences in the public schema: ALL

To do this, log in under the *postgres* user in the Server database, and then run the following script (in this script, the role is *KCSAdmin*):

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KCSAdmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KCSAdmin";
```

### 4. [Install Administration Server.](#)

After the installation finishes, the Administration Server will use the created database to store the Administration Server data. Administration Server is ready to use.

## Certificates for work with Kaspersky Security Center Linux

This section contains information about Kaspersky Security Center Linux certificates and describes how to issue and replace certificates for Kaspersky Security Center Web Console and how to renew a certificate for Administration Server if the Server interacts with Kaspersky Security Center Web Console.

### About Kaspersky Security Center certificates

Kaspersky Security Center uses the following types of certificates to enable a secure interaction between the application components:

- Administration Server certificate
- Web Server certificate
- Kaspersky Security Center Web Console certificate

By default, Kaspersky Security Center uses self-signed certificates (that is, issued by Kaspersky Security Center itself), but you can replace them with custom certificates to better meet the requirements of your organization's network and comply with the security standards. After Administration Server verifies whether a custom certificate meets all applicable requirements, this certificate assumes the same functional scope as a self-signed certificate. The only difference is that a custom certificate is not reissued automatically upon expiration. You replace certificates with custom ones by means of the `klsetsrvcert` utility or through the Administration Server properties section in Kaspersky Security Center Web Console, depending on the certificate type. When you use the `klsetsrvcert` utility, you need to specify a certificate type by using one of the following values:

- C—Common certificate for ports 13000 and 13291.
- CR—Common reserve certificate for ports 13000 and 13291.

The maximum validity period for any of the Administration Server certificates must be 397 days or less.

### Administration Server certificates

An Administration Server certificate is required for the following purposes:

- Authentication of Administration Server when connecting to Kaspersky Security Center Web Console
- Secure interaction between Administration Server and Network Agent on managed devices
- Authentication when the primary Administration Servers are connected to secondary Administration Servers

The Administration Server certificate is created automatically during installation of the Administration Server component and it is stored in the `/var/opt/kaspersky/klagent_srv/1093/cert/` folder. You specify the Administration Server certificate when you [create a response file](#) to install Kaspersky Security Center Web Console. This certificate is called common ("C").

The Administration Server certificate is valid for 397 days. Kaspersky Security Center automatically generates a common reserve ("CR") certificate 90 days before the expiration of the common certificate. The common reserve certificate is subsequently used for seamless replacement of the Administration Server certificate. When the common certificate is about to expire, the common reserve certificate is used to maintain the connection with Network Agent instances installed on managed devices. With this purpose, the common reserve certificate automatically becomes the new common certificate 24 hours before the old common certificate expires.

The maximum validity period for any of the Administration Server certificates must be 397 days or less.

If necessary, you can assign a custom certificate for the Administration Server. For example, this may be necessary for better integration with the existing PKI of your enterprise or for custom configuration of the certificate fields. When replacing the certificate, all Network Agents that were previously connected to Administration Server through SSL will lose their connection and will return "Administration Server authentication error." To eliminate this error, you will have to restore the connection after the [certificate replacement](#).

If the Administration Server certificate is lost, you must reinstall the Administration Server component, and then [restore the data](#) in order to recover it.

You can also back up the Administration Server certificate separately from other Administration Server settings in order to move Administration Server from one device to another without data loss.

## Mobile certificates

A mobile certificate ("M") is required for authentication of the Administration Server on mobile devices. You specify the mobile certificate in the Administration Server properties.

Also, a mobile reserve ("MR") certificate exists: it is used for seamless replacement of the mobile certificate. Kaspersky Security Center automatically generates this certificate 60 days before the expiration of the common certificate. When the mobile certificate is about to expire, the mobile reserve certificate is used to maintain the connection with Network Agent instances installed on managed mobile devices. With this purpose, the mobile reserve certificate automatically becomes the new mobile certificate 24 hours before the old mobile certificate expires.

If the connection scenario requires the use of a client certificate on mobile devices (connection involving two-way SSL authentication), you can generate those certificates by means of the certificate authority for auto-generated user certificates ("MCA"). Also, in the Administration Server properties, you can specify custom client certificates issued by a different certification authority, while integration with the domain Public Key Infrastructure (PKI) of your organization enables you to issue client certificates by means of your domain certification authority.

## Web Server certificate

A special type of certificate is used by Web Server, a component of Kaspersky Security Center Administration Server. This certificate is required for publishing Network Agent installation packages that you subsequently download to managed devices. For this purpose, Web Server can use various certificates.

Web Server uses one of the following certificates, in order of priority:

1. Custom Web Server certificate that you specified manually by means of Kaspersky Security Center Web Console
2. Common Administration Server certificate ("C")

## Kaspersky Security Center Web Console certificate

The Server of Kaspersky Security Center Web Console (hereinafter referred to as Web Console) has its own certificate. When you open a website, a browser verifies whether your connection is trusted. The Web Console certificate allows you to authenticate the Web Console and is used to encrypt traffic between a browser and the Web Console.

When you open the Web Console, the browser may inform you that the connection to the Web Console is not private and the Web Console certificate is invalid. This warning appears because the Web Console certificate is self-signed and automatically generated by Kaspersky Security Center. To remove this warning, you can do one of the following:

- [Replace the Web Console certificate](#) with a custom one (recommended option). Create a certificate that is trusted in your infrastructure and that meets the [requirements for custom certificates](#).
- Add the Web Console certificate to the list of trusted browser certificates. We recommend that you use this option only if you cannot create a custom certificate.

## Requirements for custom certificates used in Kaspersky Security Center Linux

The table below shows the requirements for custom [certificates specified for different components of Kaspersky Security Center Linux](#).

Requirements for Kaspersky Security Center Linux certificates

| Certificate type                                           | Requirements                                                                                                                                                                                                                                                                                                                                                                                 | Comments                                                                                                                                |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Common certificate, Common reserve certificate ("C", "CR") | Minimum key length: 2048.<br>Basic constraints: <ul style="list-style-type: none"><li>• CA: true</li><li>• Path Length Constraint: None</li></ul> Key Usage: <ul style="list-style-type: none"><li>• Digital signature</li><li>• Certificate signing</li><li>• Key encipherment</li><li>• CRL Signing</li></ul> Extended Key Usage (optional): server authentication, client authentication. | Extended Key Usage parameter is optional.<br>Path Length Constraint value may be an integer different from "None," but not less than 1. |
| Web Server certificate                                     | Extended Key Usage: server authentication.<br>The PKCS #12 / PEM container from which the certificate is specified includes the entire chain of public keys.<br>The Subject Alternative Name (SAN) of the certificate is present; that is, the value of the <code>subjectAltName</code> field is valid.                                                                                      | Not applicable.                                                                                                                         |

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                    |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
|                                                   | The certificate meets the effective requirements of web browsers imposed on server certificates, as well as the current baseline requirements of the <a href="#">CA/Browser Forum</a> .                                                                                                                                                                                                                                                         |                                                                                    |
| Kaspersky Security Center Web Console certificate | <p>The PEM container from which the certificate is specified includes the entire chain of public keys.</p> <p>The Subject Alternative Name (SAN) of the certificate is present; that is, the value of the <code>subjectAltName</code> field is valid.</p> <p>The certificate meets the effective requirements of web browsers to server certificates, as well as the current baseline requirements of the <a href="#">CA/Browser Forum</a>.</p> | Encrypted certificates are not supported by Kaspersky Security Center Web Console. |

## Reissuing the certificate for Kaspersky Security Center Web Console

Most browsers impose a limit on the validity term of a certificate. To fall within this limit, the validity term of the Kaspersky Security Center Web Console certificate is limited to 397 days. You can [replace an existing certificate](#) received from a certification authority (CA) by issuing a new self-signed certificate manually. Alternatively, you can reissue your expired Kaspersky Security Center Web Console certificate.

When you open the Kaspersky Security Center Web Console, the browser may inform you that the connection to the Kaspersky Security Center Web Console is not private and the Kaspersky Security Center Web Console certificate is invalid. This warning appears because the Web Console certificate is self-signed and automatically generated by Kaspersky Security Center Linux. To remove or prevent this warning, you can do one of the following:

- Specify a custom certificate when you reissue it (recommended option). Create a certificate that is trusted in your infrastructure and that meets the [requirements for custom certificates](#).
- Add the Kaspersky Security Center Web Console certificate to the list of trusted browser certificates after you reissue the certificate. We recommend that you use this option only if you cannot create a custom certificate.

*To reissue the expired Kaspersky Security Center Web Console certificate:*

Reinstall Kaspersky Security Center Web Console by performing one of the following:

- If you want to use the same installation file of Kaspersky Security Center Web Console, remove Kaspersky Security Center Web Console, and then [install the same Kaspersky Security Center Web Console version](#).
- If you want to use an installation file of an upgraded version, [run the upgrade command](#).

The Kaspersky Security Center Web Console certificate is reissued for another validity term of 397 days.

## Replacing certificate for Kaspersky Security Center Web Console

By default, when you install Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console), a browser certificate for the application is generated automatically. You can replace the automatically generated certificate with a custom one.



To replace the certificate for Kaspersky Security Center Web Console with a custom one:

1. [Create a new response file](#) required for the Kaspersky Security Center Web Console installation.
2. In this file, specify paths to the custom certificate file and the key file by using the `certPath` parameter and the `keyPath` parameter.
3. Reinstall Kaspersky Security Center Web Console by specifying the new response file. Do one of the following:
  - If you want to use the same installation file of Kaspersky Security Center Web Console, remove Kaspersky Security Center Web Console, and then [install the same Kaspersky Security Center Web Console version](#).
  - If you want to use an installation file of an upgraded version, [run the upgrade command](#).

Kaspersky Security Center Web Console works with the specified certificate.

## Converting a PFX certificate to the PEM format

To use a PFX certificate in Kaspersky Security Center Web Console, you must first convert it to the PEM format by using any convenient OpenSSL-based cross-platform utility.

To convert a PFX certificate to the PEM format in the Linux operating system:

1. In an OpenSSL-based cross-platform utility, execute the following commands:

```
openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
```

```
openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
```

2. Make sure that the certificate file and the private key are generated to the same directory where the .pfx file is stored.
3. Kaspersky Security Center Web Console does not support passphrase-protected certificates. Therefore, run the following command in an OpenSSL-based cross-platform utility to remove a passphrase from the .pem file:

```
openssl rsa -in key.pem -out key-without-passphrase.pem
```

Do not use the same name for the input and output .pem files.

As a result, the new .pem file is unencrypted. You do not have to enter a passphrase to use it.

The .crt and .pem files are ready to use, so you can specify them in the [Kaspersky Security Center Web Console installer](#).

## Scenario: Specifying the custom Administration Server certificate

You can assign the custom Administration Server certificate, for example, for better integration with the existing public key infrastructure (PKI) of your enterprise or for custom configuration of the certificate fields. It is useful to replace the certificate immediately after installation of Administration Server and before the quick start wizard finishes.

The maximum validity period for any of the Administration Server certificates must be 397 days or less.

## Prerequisites

The new certificate must be created in the PKCS#12 format (for example, by means of the organization's PKI) and must be issued by trusted certification authority (CA). Also, the new certificate must include the entire chain of trust and a private key, which must be stored in the file with the pfx or p12 extension. For the new certificate, the requirements listed below must be met.

Certificate type: Common certificate, common reserve certificate ("C", "CR")

Requirements:

- Minimum key length: 2048
- Basic constraints:
  - CA: true
  - Path Length Constraint: None  
Path Length Constraint value may be an integer different from "None" but not less than 1.
- Key Usage:
  - Digital signature
  - Certificate signing
  - Key encipherment
  - CRL Signing
- Extended Key Usage (EKU): server authentication and client authentication. The EKU is optional, but if your certificate contains it, the server and client authentication data must be specified in the EKU.

Certificates issued by a public CA do not have the certificate signing permission. To use such certificates, make sure that you installed Network Agent version 13 or later on distribution points or connection gateways in your network. Otherwise, you will not be able to use certificates without the signing permission.

## Stages

Specifying the Administration Server certificate proceeds in stages:

### 1 Replacing the Administration Server certificate

Use the command-line [ksetsrvcert utility](#) for this purpose.

### 2 Specifying a new certificate and restoring connection of Network Agents to the Administration Server

When the certificate is replaced, all Network Agents that were previously connected to Administration Server through SSL lose their connection and return "Administration Server authentication error." To specify the new certificate and restore the connection, use the command-line [klmover utility](#).

## Results

When you finish the scenario, the Administration Server certificate is replaced and the server is authenticated by Network Agents on the managed devices.

## Replacing the Administration Server certificate by using the klsetsrvcert utility

To replace the Administration Server certificate:

From the command line, run the following utility:

```
klsetsrvcert [-t <type> {-i <inputfile> [-p <password>] [-o <chkopt>] | -g <dnsname>}] [-f <time>][-r <calistfile>][-l <logfile>]
```

You do not need to download the klsetsrvcert utility. It is included in the Kaspersky Security Center Linux distribution kit. It is not compatible with previous Kaspersky Security Center Linux versions.

The description of the klsetsrvcert utility parameters is presented in the table below.

Values of the klsetsrvcert utility parameters

| Parameter      | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -t <type>      | Type of certificate to be replaced. Possible values of the <type> parameter: <ul style="list-style-type: none"><li>• C—Replace the common certificate for ports 13000 and 13291.</li><li>• CR—Replace the common reserve certificate for ports 13000 and 13291.</li></ul>                                                                                                                                                                                                       |
| -f <time>      | Schedule for changing the certificate, using the format "DD-MM-YYYY hh:mm" (for ports 13000 and 13291).<br>Use this parameter if you want to replace the common or common reserve certificate before it expires.<br>Specify the time when managed devices must synchronize with Administration Server on a new certificate.                                                                                                                                                     |
| -i <inputfile> | Container with the certificate and a private key in the PKCS#12 format (file with the .p12 or .pfx extension).                                                                                                                                                                                                                                                                                                                                                                  |
| -p <password>  | Password used for protection of the p12 container.<br>The certificate and a private key are stored in the container, therefore, the password is required to decrypt the file with the container.                                                                                                                                                                                                                                                                                |
| -o <chkopt>    | Certificate validation parameters (semicolon separated).<br>To use a custom certificate without signing permission, specify -o NoCA in the klsetsrvcert utility. This is useful for certificates issued by a public CA.<br>To change encryption key length for certificate types C or CR, specify -o RsaKeyLen: <key length> in the klsetsrvcert utility, where <key length> parameter is the required key length value. Otherwise, the current certificate key length is used. |

|                    |                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------|
| -g<br><dnsname>    | A new certificate will be created for the specified DNS name.                              |
| -r<br><calistfile> | Trusted root Certificate Authority list, format PEM.                                       |
| -l<br><logfile>    | Results output file. By default, the output is redirected into the standard output stream. |

For example, to specify the [custom Administration Server certificate](#), use the following command:

```
klsetsrvcert -t C -i <inputfile> -p <password> -o NoCA
```

After the certificate is replaced, all Network Agents connected to Administration Server through SSL lose their connection. To restore it, use the command-line [klmover utility](#).

To avoid losing the Network Agents connections, use the following commands:

1. To install the new certificate,

```
klsetsrvcert -t CR -i <inputfile> -p <password> -o NoCA
```

2. To specify the date when the new certificate will be applied,

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

where "DD-MM-YYYY hh:mm" is the date 3–4 weeks later than the current date. The time shift for changing the certificate to the new one will allow the new certificate to be distributed to all Network Agents.

## Connecting Network Agents to Administration Server by using the klmover utility

After you replace the Administration Server certificate by using the command-line [klsetsrvcert utility](#), you need to establish the SSL connection between Network Agents and Administration Server because the connection is broken.

*To specify the new Administration Server certificate and restore the connection:*

From the command line, run the following utility:

```
klmover [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-noss1] [-cert <path to certificate file>]
```

This utility is automatically copied to the Network Agent installation folder, when Network Agent is installed on a client device.

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** also enables password protection for the Removal tool for Kaspersky Security Center Web Console (cleaner.exe).

The description of the klmover utility parameters is presented in the table below.

Values of the klmover utility parameters

| Parameter                        | Value                                                                                                                                                                            |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -address <server address>        | Address of the Administration Server for connection.<br>You can specify an IP address or the DNS name.                                                                           |
| -pn <port number>                | Number of the port through which non-encrypted connection to the Administration Server is established.<br>The default port number is 14000.                                      |
| -ps <SSL port number>            | Number of the SSL port through which encrypted connection to the Administration Server is established by using SSL.<br>The default port number is 13000.                         |
| -noss1                           | Use non-encrypted connection to the Administration Server.<br>If the key is not in use, Network Agent is connected to the Administration Server by using encrypted SSL protocol. |
| -cert <path to certificate file> | Use the specified certificate file for authentication of access to Administration Server.                                                                                        |

## Defining a shared folder

After Administration Server installation, you can specify the location of the shared folder, in the Administration Server properties. By default, the shared folder is created on the device with Administration Server. However, in some cases (such as high load or a need for access from an isolated network), it is useful to locate the shared folder on a dedicated file resource.

The shared folder is used occasionally in Network Agent deployment.

Case sensitivity for the shared folder must be disabled.

## Signing in to Kaspersky Security Center Web Console and signing out

You can sign in to Kaspersky Security Center Web Console after you [install the Administration Server and Web Console Server](#). You must know the web address of the Administration Server and the port number specified during installation (by default, the port is 8080). In your browser, JavaScript must be enabled.

*To sign in to Kaspersky Security Center Web Console:*

1. In your browser, go to <Administration Server web address>:<Port number>.

The sign-in page is displayed.

2. If you added several trusted servers, in the Administration Servers list select the Administration Server that you want to connect to.

If you only added one Administration Server, the Administration Servers list is locked.

3. Do one of the following:

- To sign in to the Administration Server with a domain user account, enter the user name and password of the domain user.

You can enter the user name of the domain user in one of the following formats:

- Username@dns.domain
- NTDOMAIN\Username

Before you sign in with a domain user account, [poll the domain controller](#) to obtain the list of domain users.

- To sign in to the Administration Server by specifying the administrator's user name and password, enter the user name and password of the internal user.
- If one or more virtual Administration Servers are created on the Server and you want to sign in to a virtual Server:
  - a. Click **Show virtual Server options**.
  - b. Type the virtual Administration Server name that you specified while [creating the virtual Server](#).
  - c. Enter the user name and password of the administrator who has rights on the virtual Administration Server.

4. Click the **Sign in** button.

After sign-in, the dashboard is displayed, containing the language and theme that you used last time. You can navigate through Kaspersky Security Center Web Console and use it to work with Kaspersky Security Center Linux.

## Signing out

*To sign out of Kaspersky Security Center Web Console,*

In the main menu, go to your account settings, and then select **Sign out**.

Kaspersky Security Center Web Console is closed, and the sign-in page is displayed.

## Changing the language of the Kaspersky Security Center Web Console interface

You can select the language of the Kaspersky Security Center Web Console interface.

*To change the interface language:*

1. In the main menu, go to **Settings** → **Language**.
2. Select one of the supported localization languages.

## Configuring the MySQL x64 server for working with Kaspersky Security Center Linux

If you use the MySQL server for Kaspersky Security Center, enable support of InnoDB and MEMORY storage and of UTF-8 and UCS-2 encodings.

### Recommended settings for the my.cnf file

For more details about DBMS configuring, refer also to the [account configuring](#) procedure. For information about DBMS installation, refer to the [DBMS installation](#) procedure.

*To configure the my.cnf file:*

1. Open the my.cnf file in a text editor.
2. Add the following lines into the [mysqld] section of the my.ini file:

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=the real value must be no less than 80% of the expected KAV
database size
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (in most cases, the server uses small transactions)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Note that the memory specified in the `innodb_buffer_pool_size` value is allocated at server startup. If the database size is smaller than the specified buffer size, only the required memory is allocated. The actual size of allocated memory is approximately 10 percent greater than the specified buffer size. Refer to the [MySQL documentation](#) for details.

It is recommended to use the parameter value `innodb_flush_log_at_trx_commit = 0`, because the values "1" or "2" negatively affect the operating speed of MySQL.

## Quick start wizard

Kaspersky Security Center Linux allows you to adjust a minimum selection of settings required to build a centralized management system for protecting your network against security threats. This configuration is performed through the quick start wizard. When the wizard is running, you can make the following changes to the application:

- Add key files or enter activation codes that can be automatically distributed to devices within administration groups.
- Set up email delivery of notifications of events that occur during operation of Administration Server and managed applications (successful notification delivery requires that the Messenger service run on the Administration Server and all recipient devices).
- Create a protection policy for workstations and servers, as well as malware scan tasks, update download tasks, and data backup tasks, for the top level of the hierarchy of managed devices.

The quick start wizard creates policies only for those applications whose **Managed devices** folder does not contain policies. The quick start wizard does not create tasks if tasks with the same names have already been created for the top level in the hierarchy of managed devices.

The application automatically prompts you to run the quick start wizard after Administration Server installation, at the first connection to it. You can also start the quick start wizard manually at any time.

*To start the quick start wizard manually:*

1. In the main menu, click the settings icon (⚙️) next to the name of the Administration Server.  
The Administration Server properties window opens.
2. On the **General** tab, select the **General** section.
3. Click **Start quick start wizard**.

The wizard prompts you to perform initial configuration of the Administration Server. Follow the instructions of the wizard. Proceed through the wizard by using the **Next** button.

## Step 1. Specifying the internet connection settings

Specify the internet access settings for Administration Server. You must configure internet access to use Kaspersky Security Network and to download updates of anti-virus databases for Kaspersky Security Center Linux and managed Kaspersky applications.

Enable the **Use proxy server** option if you want to use a proxy server when connecting to the internet. If this option is enabled, the fields are available for entering settings. Specify the following settings for a proxy server connection:

- [Address](#) ⓘ

Address of the proxy server used for Kaspersky Security Center Linux connection to the internet.

- [Port number](#) ⓘ

Number of the port through which Kaspersky Security Center Linux proxy connection will be established.

- [Bypass proxy server for local addresses](#) ⓘ



No proxy server will be used to connect to devices in the local network.

- [Proxy server authentication](#) 

If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

This entry field is available if the **Use proxy server** check box is selected.

- [User name](#) 

User account under which connection to the proxy server is established (this field is available if the **Proxy server authentication** check box is selected).

- [Password](#) 

Password set by the user under whose account the proxy server connection is established (this field is available if the **Proxy server authentication** check box is selected).

To see the entered password, click and hold the **Show** button for as long as you require.

You can [configure internet access](#) later, separately from the quick start wizard.

## Step 2. Downloading required updates

The required updates are downloaded from the Kaspersky servers automatically.

## Step 3. Selecting the assets to secure

Select the protection areas and operating systems that are in use on your network. When you select these options, you specify the filters for application management plug-ins and distribution packages on Kaspersky servers that you can download to install on client devices on your network. Select the options:

- [Areas](#) 

You can select the following protection scopes:

- **Workstations**
- **File servers and storage**
- **Virtualization**
- **Embedded systems**
- **Industrial networks**
- **Industrial endpoints**

- [Operating systems](#) 

You can select the following platforms:

- Microsoft Windows
- macOS
- Android
- Linux
- Other

For information about supported operating systems, refer to Hardware and software requirements for Kaspersky Security Center Web Console.

You can select the Kaspersky application packages from the list of available packages later, separately from the quick start wizard. To simplify the search for the required packages, you can filter the list of available packages by various criteria.

## Step 4. Selecting encryption in solutions

The **Encryption in solutions** window is displayed only if you have selected **Workstations** as a protection scope.

Kaspersky Endpoint Security for Windows includes encryption tools for information stored on Windows-based client devices. These encryption tools have the Advanced Encryption Standard (AES) implemented with a 256-bit or 56-bit key length.

Download and usage of the distribution package with a 256-bit key length must be performed in compliance with applicable laws and regulations. To download a distribution package of Kaspersky Endpoint Security for Windows that is valid for the needs of your organization, consult the legislation of the country where the client devices of your organization are located.

In the **Encryption in solutions** window, select one of the following encryption types:

- Lite encryption. This encryption type uses a 56-bit key length.
- Strong encryption. This encryption type uses a 256-bit key length.

You can select the distribution package for Kaspersky Endpoint Security for Windows with the required encryption type later, separately from the quick start wizard.

## Step 5. Configuring installation of plug-ins for managed applications

Select plug-ins for managed applications to install. A list of plug-ins located on Kaspersky servers is displayed. The list is filtered according to the options selected on the previous step of the wizard. By default, a full list includes plug-ins of all languages. To display only plug-in of specific language, use filter. The list of plug-ins includes the following columns:

- [Area to secure](#) 

The selected areas to secure are displayed in this column.

- [Type](#)

The plug-in types are displayed in this column.

- [Name](#)

The plug-ins depending of the protection areas and platforms that you have selected on the previous step are selected.

- [Version](#)

The list includes plug-ins of all the versions placed on Kaspersky servers. By default, the plug-ins of the latest versions are selected.

- [Latest version](#)

This column indicates whether a plug-in version is the latest. If **true** value is displayed, the corresponding plug-in is of the latest version. If **false** value is displayed, the corresponding plug-in has a later version.

- [Operating system](#)

This column displays plug-ins operating systems.

- [Language](#)

By default, the localization language of a plug-in is defined by the Kaspersky Security Center Linux language that you have selected at installation. You can specify other languages in **Show the Administration Console localization language** or drop-down list.

After the plug-ins are selected, click **Next** to start installation.

You can install management plug-ins for Kaspersky applications manually, separately from the quick start wizard.

The quick start wizard automatically installs the selected plug-ins. To install some plug-ins, you must accept the terms of the EULA. Read the text of EULA displayed, select the **I agree to use Kaspersky Security Network** check box and click the **Install** button. If you do not accept the terms of the EULA, the plug-in is not installed.

When all the selected plug-ins are installed, the quick start wizard automatically takes you to the next step.

## Step 6. Downloading distribution packages and creating installation packages

Select the distribution packages to download.

Distributives of managed applications may require a specific minimum version of Kaspersky Security Center Linux to be installed.

After you have selected an encryption type for Kaspersky Endpoint Security for Windows, a list of distribution packages of both encryption types is displayed. A distribution package with the selected encryption type is selected in the list. You can select distribution packages of any encryption type. The distribution package language corresponds to the Kaspersky Security Center Linux language. If an application distribution package for the Kaspersky Security Center Linux language does not exist, the English distribution package is selected.

To finish downloading of some distribution packages you must accept EULA. When you click the **Accept** button, the text of EULA is displayed. To proceed to the next step of the wizard, you must accept the terms and conditions of the EULA and the terms and conditions of Kaspersky Privacy Policy. If you do not accept the terms and conditions, the downloading of the package is canceled.

After you have accepted the terms and conditions of the EULA and the terms and conditions of Kaspersky Privacy Policy, the downloading of the distribution packages continues. Later, you can use installation packages to deploy Kaspersky applications on client devices.

## Step 7. Configuring Kaspersky Security Network

Specify the settings for relaying information about Kaspersky Security Center Linux operations to the Kaspersky Security Network knowledge base. Select one of the following options:

- [I agree to use Kaspersky Security Network](#) 

Kaspersky Security Center Linux and managed applications installed on client devices will automatically transfer their operation details to [Kaspersky Security Network](#). Participation in Kaspersky Security Network ensures faster updates of databases containing information about viruses and other threats, which ensures a faster response to emergent security threats.

- [I do not agree to use Kaspersky Security Network](#) 

Kaspersky Security Center Linux and managed applications will provide no information to Kaspersky Security Network.

If you select this option, the use of Kaspersky Security Network will be disabled.

You can [set up access to Kaspersky Security Network \(KSN\)](#) later, separately from the quick start wizard.

## Step 8. Selecting the application activation method

Select one of the following Kaspersky Security Center Linux activation options:

- [By entering your activation code](#) 

*Activation code* is a unique sequence of 20 alphanumeric characters. You enter an activation code to add a key that activates Kaspersky Security Center Linux. You receive the activation code through the email address that you specified after purchasing Kaspersky Security Center.

To activate the application by using the activation code, you need internet access to establish connection with Kaspersky activation servers.

If you have selected this activation option, you can enable the **Automatically deploy license key to managed devices** option.

If this option is enabled, the license key will be deployed automatically to managed devices.

If this option is disabled, you can deploy license key to managed devices later in the **Operations** → **Licensing** → **Kaspersky licenses** section of the main menu.

- [By specifying a key file](#) 

*Key file* is a file with the .key extension provided to you by Kaspersky. A key file is intended for adding a key that activates the application.

You receive your key file through the email address that you specified after purchasing Kaspersky Security Center.

To activate the application using a key file, you do not have to connect to Kaspersky activation servers.

If you have selected this activation option, you can enable the **Automatically deploy license key to managed devices** option.

If this option is enabled, the license key will be deployed automatically to managed devices.

If this option is disabled, you can deploy license key to managed devices later in the **Operations** → **Licensing** → **Kaspersky licenses** section of the main menu.

- By postponing the application activation

If you chose to postpone application activation, you can add a license key later at any time by selecting **Operations** → **Licensing**.

When working with Kaspersky Security Center deployed from a paid AML or for a usage-based monthly billed SKU, you cannot specify a key file or enter a code.

## Step 9. Creating a basic network protection configuration

You can check a list of policies and tasks that are created.

Wait for the creation of policies and tasks to complete before proceeding to the next step of the wizard.

## Step 10. Configuring email notifications

Configure the delivery of notifications about events registered during the operation of Kaspersky applications on client devices. These settings will be used as the default settings for application policies.

To configure the delivery of notifications about events occurring in Kaspersky applications, use the following settings:

- [Recipients \(email addresses\)](#) <sup>?</sup>

The email addresses of users to whom the application will send notifications. You can enter one or more addresses; if you enter more than one address, separate them with a semicolon.

- [SMTP server address](#) <sup>?</sup>

The address or addresses of your organization's mail servers.

If you enter more than one address, separate them with a semicolon. You can use the following values:

- IPv4 or IPv6 address
- DNS name of the SMTP server

- [SMTP server port](#) <sup>?</sup>

Communication port number of the SMTP server. If you use several SMTP servers, the connection to them is established through the specified communication port. The default port number is 25.

- [Use ESMTP authentication](#) <sup>?</sup>

Enables support of ESMTP authentication. When the check box is selected, in the **User name** and **Password** fields you can specify the ESMTP authentication settings. By default, this check box is cleared.

You can test the new email notification settings by clicking the **Send test message** button.

## Step 11. Closing the quick start wizard

To close the wizard, click the **Finish** button.

After you have completed the quick start wizard, you can run the [Protection deployment wizard](#) to automatically install anti-virus applications or Network Agent on devices on your network.

## Protection deployment wizard

To install Kaspersky applications, you can use the Protection deployment wizard. The Protection deployment wizard enables remote installation of applications either through specially created installation packages or directly from a distribution package.

The Protection deployment wizard performs the following actions:

- Downloads an installation package for application installation (if it was not created earlier). The installation package is located at **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**.

If you want to install Network Agent on devices with the SUSE Linux Enterprise Server 15 operating system, [install the insserv-compatible package](#) first to configure Network Agent.

## Starting Protection deployment wizard

You can start the Protection deployment wizard manually at any time.

*To start the Protection deployment wizard manually,*

In the main menu, go to **Discovery & deployment** → **Deployment & assignment** → **Protection deployment wizard**.

The Protection deployment wizard starts. Proceed through the wizard by using the **Next** button.

## Step 1. Selecting the installation package

Select the installation package of the application that you want to install.

If the installation package of the required application is not listed, click the **Add** button and then select the application from the list.

## Step 2. Selecting a method for distribution of key file or activation code

Select a method for the distribution of the key file or the activation code:

- [Do not add license key to installation package](#) 

The key is automatically distributed to all devices with which it is compatible:

- If automatic distribution has been enabled in the key properties.
- If the **Add key** task has been created.

- [Add license key to installation package](#) 

The key is distributed to devices together with the installation package.

We do not recommend that you distribute the key using this method because the shared Read access rights are enabled to the repository of installation packages.

If the installation package already includes a key file or an activation code, this window is displayed, but it only contains the license key information.

## 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, this option is enabled.

- [Using operating system resources through distribution points](#) ⓘ



If this option is enabled, installation packages are transmitted to client devices using operating system tools through distribution points. You can select this option if there is at least one distribution point on the network.

If the **Using Network Agent** option is enabled, the files are delivered using operating system tools only if Network Agent tools are unavailable.

By default, this option is enabled for remote installation tasks that have been created on a virtual Administration Server.

The only way to install an application for Windows (including Network Agent for Windows) on a device that does not have Network Agent installed is by using a Windows-based distribution point. Therefore, when you install a Windows application:

- Select this option.
- Ensure that a distribution point is assigned for the target client devices.
- Ensure the distribution point is Windows-based.

- [Using operating system resources through Administration Server](#) ⓘ

If this option is enabled, files are transmitted to client devices by using operating system tools of client devices through the Administration Server. You can enable this option if no Network Agent is installed on the client device, but the client device is in the same network as the Administration Server.

By default, this option is enabled.

Define the additional setting:

- [Do not re-install application if it is already installed](#) ⓘ

If this option is enabled, the selected application will not be re-installed if it has already been installed on this client device.

If this option is disabled, the application will be installed anyway.

By default, this option is enabled.

## Step 6. Removing incompatible applications before installation

This step is only present if the application that you deploy is known to be incompatible with some other applications.

Select the option if you want Kaspersky Security Center Linux to automatically remove applications that are incompatible with the application you deploy.

The list of incompatible applications is also displayed.

If you do not select this option, the application will only be installed on devices that have no incompatible applications.

## Step 7. Moving devices to Managed devices

Specify whether devices must be moved to an administration group after Network Agent installation.

- [Do not move devices](#) <sup>?</sup>

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](#) <sup>?</sup>

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 8. Selecting accounts to access devices

If necessary, add the accounts that will be used to start the remote installation task:

- [No account required \(Network Agent installed\)](#) <sup>?</sup>

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 \(Network Agent is not used\)](#) <sup>?</sup>

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 to install the application.

To specify the user account under which the application installer will be run, click the **Add** button, select **Local 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.

## Step 9. Starting installation

This page is the final step of the wizard. At this step, the **Remote installation task** has been successfully created and configured.

By default, the **Run the task after the wizard finishes** option is not selected. If you select this option, the **Remote installation task** will start immediately after you complete the wizard. If you do not select this option, the **Remote installation task** will not start. You can later start this task manually.

Click **OK** to complete the final step of the Protection deployment wizard.

# Upgrading Kaspersky Security Center Linux

You can install version 15 of Administration Server on a device that has an earlier version of Administration Server installed (starting from version 13). When upgrading to version 15, all data and settings from the previous version of Administration Server are preserved.

Before upgrading Kaspersky Security Center Linux, ensure that you use the versions of the operating system and DBMS that are [supported by version 15 of Administration Server](#). If necessary, you can [move Administration Server to another device](#) with later versions of the operating system and DBMS.

You can upgrade a version of Administration Server by using one of the following methods:

- By using the [Kaspersky Security Center Linux installation file](#)
- By creating the [Administration Server data backup](#), installing a new Administration Server version, and restoring the Administration Server data from the backup

During the upgrade, concurrent use of the DBMS by Administration Server and another application is strictly forbidden.

If your network includes several Administration Servers, you have to upgrade every Server manually. Kaspersky Security Center Linux does not support centralized upgrade.

Also, you have to [upgrade Kaspersky Security Center Web Console](#) to a new version.

When you upgrade Kaspersky Security Center Linux from a previous version, all the installed plug-ins of supported Kaspersky applications are kept. Administration Server plug-in and Network Agent plug-in are upgraded automatically. We recommend [creating a backup copy of the Administration Server data](#) before starting the upgrade.

## Upgrading Kaspersky Security Center Linux by using the installation file

To upgrade Administration Server from a previous version (starting from version 13) to version 15, you can install a new version over an earlier one by using the Kaspersky Security Center Linux installation file.

*To upgrade an earlier version of Administration Server to version 15 by using the installation file:*

1. Download the Kaspersky Security Center Linux installation file with a full package for version 15 from the Kaspersky website:
  - For devices running an RPM-based operating system—`ksc64-<version number>.x86_64.rpm`
  - For devices running a Debian-based operating system—`ksc64_<version number>_amd64.deb`
2. Upgrade the installation package by using a package manager that you use on your Administration Server. For example, you can use the following commands in the command-line terminal under an account with root privileges:
  - For devices running an RPM-based operating system:

```
$ sudo rpm -Uvh --nodeps --force ksc64-<version number>.x86_64.rpm
```

- For devices running a Debian-based operating system:  
\$ sudo dpkg -i ksc64\_<version number>\_amd64.deb

After the command has been successfully executed, the /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl script is created. The message about that is displayed in the terminal.

3. Run the /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl script to configure the upgraded Administration Server.
4. Read the License Agreement and Privacy Policy, which appear in the command-line terminal. If you agree with all of the terms of the License Agreement and Privacy Policy:
  - a. Enter 'Y' to confirm that you have fully read, understood, and accept the terms and conditions of the EULA.
  - b. Enter 'Y' again to confirm that you have fully read, understood, and accept the Privacy Policy that describes the handling of data.

Installation of the application on your device will continue after you have entered 'Y' twice.

5. Enter '1' to select the standard Administration Server installation mode.

The picture below shows the last two steps.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

Accepting the terms of the EULA and the Privacy Policy, and selecting the standard Administration Server installation mode in the command-line terminal

Next, the script configures and finishes upgrading the Administration Server. During the upgrade, you cannot change the Administration Server settings adjusted before the upgrade.

6. For devices on which the earlier version of Network Agent was installed, create and run the task for remote installation of the new version of Network Agent.

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

After completion of the remote installation task, the Network Agent version is upgraded.

## Upgrading Kaspersky Security Center Linux through backup

To upgrade Administration Server from a previous version (starting from version 13) to version 15, you can create a backup of the Administration Server data and restore this data after installing Kaspersky Security Center Linux of a new version. If problems occur during installation, you can restore the previous version of Administration Server by using the backup of the Administration Server data created before the upgrade.

To upgrade an earlier version of Administration Server to version 15 through backup:

1. Before the upgrade, [back up the Administration Server data](#) with an older version of the application.
2. Uninstall the older version of Kaspersky Security Center Linux.
3. [Install Kaspersky Security Center Linux version 15](#) on the former Administration Server.
4. [Restore the Administration Server data](#) from the backup created before the upgrade.
5. For devices on which the earlier version of Network Agent was installed, create and run the task for remote installation of the new Network Agent version.

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

After completion of the remote installation task, the Network Agent version is upgraded.

## Upgrading Kaspersky Security Center Linux on the Kaspersky Security Center Linux failover cluster nodes

You can install Administration Server version 15 on every Kaspersky Security Center Linux failover cluster node where the Administration Server with an earlier version is installed (starting from version 14). When upgrading to version 15, all data and settings from the previous version of Administration Server are preserved.

If you previously installed Kaspersky Security Center Linux on devices locally, you can also upgrade Kaspersky Security Center Linux on these devices by using the [installation file](#) or [through backup](#).

To upgrade Kaspersky Security Center Linux on the Kaspersky Security Center Linux failover cluster nodes:

1. Download the Kaspersky Security Center Linux installation file with a full package for version 15 from the Kaspersky website:
  - For devices running an RPM-based operating system—`ksc64-<version number>-<build number>.x86_64.rpm`
  - For devices running a Debian-based operating system—`ksc64_<version number>-<build number>_amd64.deb`
2. [Stop the cluster](#).
3. On the active node of the cluster upgrade the installation package by using a package manager that you use on your Administration Server.

For example, you can use the following commands in the command-line terminal under an account with root privileges:

- For devices running an RPM-based operating system:

```
$ sudo rpm -Uvh --nodeps --force ksc64-<version number>-<build number>.x86_64.rpm
```
- For devices running a Debian-based operating system:

```
$ sudo dpkg -i ksc64_<version number>-<build number>_amd64.deb
```

After the command has been successfully executed, the `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` script is created. The message about that is displayed in the terminal.

4. Run the `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` script to configure the upgraded Administration Server.
5. Read the License Agreement and Privacy Policy, which appear in the command-line terminal. If you agree with all of the terms of the License Agreement and Privacy Policy:
  - a. Enter 'Y' to confirm that you have fully read, understood, and accept the terms and conditions of the EULA.
  - b. Enter 'Y' again to confirm that you have fully read, understood, and accept the Privacy Policy that describes the handling of data.

Installation of the application on your device will continue after you have entered 'Y' twice.

6. Select the node on which you are upgrading by entering '2'.

The picture below shows the last two steps.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

Accepting the terms of the EULA and the Privacy Policy, and selecting the installation mode in the command-line terminal

Next, the script configures and finishes upgrading the Administration Server. During the upgrade, you cannot change the Administration Server settings adjusted before the upgrade.

7. Perform steps 3-5 on the passive node.

At step 6, enter '3' to select the node.

8. [Start the cluster](#).

Note that you can start the cluster on any node. If you start the cluster on the passive node, it becomes the active node.

As a result, you installed the Administration Server of the latest version on the Kaspersky Security Center Linux failover cluster nodes.

## Upgrading Kaspersky Security Center Web Console

This article describes how to upgrade Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) on devices running the Linux operating system.

If you need to upgrade Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode, follow the [instructions specific for Astra Linux](#).

Use one of the following installation files that corresponds to the Linux distribution installed on your device:

- For Debian—ksc-web-console-[build\_number].x86\_64.deb
- For RPM-based operating systems—ksc-web-console-[build\_number].x86\_64.rpm
- For ALT 8 SP—ksc-web-console-[build\_number]-alt8p.x86\_64.rpm

You receive the installation file by downloading it from the Kaspersky website.

*To upgrade Kaspersky Security Center Web Console:*

1. Make sure that the device on which you want to upgrade Kaspersky Security Center Web Console is running one of the supported Linux distributions.
2. Read and accept the End User License Agreement (EULA). If the Kaspersky Security Center Linux distribution kit does not include a TXT file with the text of the EULA, you can download the file from the [Kaspersky website](#). If you do not accept the terms of the License Agreement, do not upgrade Kaspersky Security Center Web Console by using the installation file.
3. Use the same [response file](#) that you prepared before installing Kaspersky Security Center Web Console. The response file name is ksc-web-console-setup.json, and the file location is /etc/ksc-web-console-setup.json. If the response file does not exist, [create a new response file](#) that contains the parameters for connecting Kaspersky Security Center Web Console to Administration Server. Name the file ksc-web-console-setup.json, and then place it in the /etc directory.

Example of a response file containing a minimal set of parameters, and the default address and port:

```
{
 "address": "127.0.0.1",
 "port": 8080,
 "trusted":
 "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/k1server.cer|KSC
 Server",
 "acceptEula": true
}
```

If you want to upgrade Kaspersky Security Center Web Console connected to Administration Server installed on the Kaspersky Security Center Linux failover cluster nodes, in the [response file](#), specify the trusted installation parameter to allow the Kaspersky Security Center Linux failover cluster to connect to Kaspersky Security Center Web Console. The string value of this parameter has the following format:

```
"trusted": "server address|port|certificate path|server name"
```

Specify the components of the trusted installation parameter:

- **Administration Server address.** If you created a secondary network adapter when [preparing the cluster nodes](#), use the IP address of the adapter as the Kaspersky Security Center Linux failover cluster address. Otherwise, specify the IP address of the third-party load balancer that you use.
- **Administration Server port.** The OpenAPI port that Kaspersky Security Center Web Console uses to connect to Administration Server (default value is 13299).
- **Administration Server certificate.** The Administration Server certificate is located in the shared data storage of the [Kaspersky Security Center Linux failover cluster](#). The default path to the certificate file is: <shared data folder>\1093\cert\k1server.cer. Copy the certificate file from the shared data storage to the



device where you install Kaspersky Security Center Web Console. Specify the local path to the Administration Server certificate.

- **Administration Server name.** The Kaspersky Security Center Linux failover cluster name that will be displayed in the login window of Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console cannot be upgraded by using the same .rpm installation file. If you want to change the settings in a response file and use this file to reinstall the application, you must first remove the application, and then install it again with the new response file.

4. Under an account with root privileges, use the command line to run the setup file with the .deb or .rpm extension, depending on your Linux distribution.

To upgrade from a previous version of Kaspersky Security Center Web Console, run one of the following commands:

- For devices running an RPM-based operating system:  

```
$ sudo rpm -Uvh --nodeps --force ksc-web-console-[build_number].x86_64.rpm
```
- For devices running a Debian-based operating system:  

```
$ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
```

This starts unpacking the setup file. Please wait until the installation is complete.

5. Restart all of the Kaspersky Security Center Web Console services by running the following command:  

```
$ sudo systemctl restart KSC*
```

When the upgrade is complete, you can use your browser to [open and log in to Kaspersky Security Center Web Console](#).

## Upgrading Kaspersky Security Center Web Console on Astra Linux in the closed software environment mode

This article describes how to upgrade Kaspersky Security Center Web Console Server (also referred to as Kaspersky Security Center Web Console) on the Astra Linux Special Edition operating system.

*To upgrade Kaspersky Security Center Web Console:*

1. Make sure that the device on which you want to upgrade Kaspersky Security Center Web Console is running one of the supported Linux distributions.
2. Read and accept the End User License Agreement (EULA). If the Kaspersky Security Center Linux distribution kit does not include a TXT file with the text of the EULA, you can download the file from the [Kaspersky website](#). If you do not accept the terms of the License Agreement, do not upgrade Kaspersky Security Center Web Console by using the installation file.
3. Use the same [response file](#) that you prepared before installing Kaspersky Security Center Web Console. The response file name is ksc-web-console-setup.json, and the file location is /etc/ksc-web-console-setup.json.  
If the response file does not exist, [create a new response file](#) that contains the parameters for connecting Kaspersky Security Center Web Console to Administration Server. Name the file ksc-web-console-setup.json, and then place it in the /etc directory.

Example of a response file containing a minimal set of parameters, and the default address and port:



```
{
 "address": "127.0.0.1",
 "port": 8080,
 "trusted":
 "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
 Server",
 "acceptEula": true
}
```

4. Ensure that in the `/etc/digsig/digsig_initramfs.conf` file, the `DIGSIG_ELF_MODE` parameter is specified as follows:

```
DIGSIG_ELF_MODE=1
```

5. Ensure that the `astra-digsig-oldkeys` compatibility package is installed.

If this package is not installed, run the following command:

```
apt install astra-digsig-oldkeys
```

6. Create a directory for the application key, if it does not exist:

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

7. Place the application key `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` in the directory created in the previous step:

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

If the Kaspersky Security Center Linux distribution kit does not include the `kaspersky_astra_pub_key.gpg` application key, you can download it by clicking the link:

[https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky\\_astra\\_pub\\_key.gpg](https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg).

8. Update the RAM disks:

```
update-initramfs -u -k all
```

Reboot the system.

9. Under an account with root privileges, use the command line to run the setup file. You receive the setup file by downloading it from the Kaspersky website.

To upgrade from a previous version of Kaspersky Security Center Web Console, run the following command:

```
$ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
```

This starts unpacking the setup file. Please wait until the installation is complete.

10. Restart all of the Kaspersky Security Center Web Console services by running the following command:

```
$ sudo systemctl restart KSC*
```

When the upgrade is complete, you can use your browser to [open and log in to Kaspersky Security Center Web Console](#).

# Migration to Kaspersky Security Center Linux

Following this scenario, you can transfer the administration group structure, included managed devices and other group objects (policies, tasks, global tasks, tags, and device selections) from Kaspersky Security Center Windows under management of Kaspersky Security Center Linux.

Limitations:

- Migration is only possible from Kaspersky Security Center 14.2 Windows to Kaspersky Security Center 15.0 Linux.
- You can perform this scenario only by using Kaspersky Security Center Web Console.

Before you begin, learn more about features and limitations of Kaspersky Security Center Linux:

- [Functional differences between Kaspersky Security Center Windows and Kaspersky Security Center Linux](#)
- [List of Kaspersky applications supported by Kaspersky Security Center Linux](#)

## Stages

The migration scenario proceeds in stages:

### 1 Choose a migration method

You migrate to Kaspersky Security Center Linux through the Migration wizard. The Migration wizard steps depend on whether or not Administration Servers of Kaspersky Security Center Windows and Kaspersky Security Center Linux are arranged into a hierarchy:

- Migration by using a hierarchy of Administration Servers  
Choose this option if Administration Server of Kaspersky Security Center Windows acts as secondary to Administration Server of Kaspersky Security Center Linux. You manage the migration process and switch between Servers within a single instance of Kaspersky Security Center Web Console. If you prefer this option, you can arrange Administration Servers into a hierarchy to simplify the migration procedure. To do this, create the hierarchy before starting the migration.
- Migration by using an export file (ZIP archive)  
Choose this option if Administration Servers of Kaspersky Security Center Windows and Kaspersky Security Center Linux are not arranged into a hierarchy. You manage the migration process with two instances of Kaspersky Security Center Web Console—an instance for Kaspersky Security Center Windows and another one for Kaspersky Security Center Linux. In this case, you will use the export file that you created and downloaded during the [export from Kaspersky Security Center Windows](#) and [import this file to Kaspersky Security Center Linux](#).

### 2 Export data from Kaspersky Security Center Windows

Open Kaspersky Security Center Windows, and then run the [Migration wizard](#).

### 3 Import data to Kaspersky Security Center Linux

Continue the Migration wizard to [import the exported data to Kaspersky Security Center Linux](#). If the Servers are arranged into a hierarchy, the import starts automatically after a successful export within the same wizard. If the Servers are not arranged into a hierarchy, you continue the Migration wizard after switching to Kaspersky Security Center Linux.

### 4 Perform additional actions to transfer objects and settings from Kaspersky Security Center Windows to Kaspersky Security Center Linux manually (optional step)

You might also want to transfer the objects and settings that cannot be transferred through the Migration wizard. For example, you could additionally do the following:

- Transfer the license keys used by [Administration Server](#) and managed applications
- Configure global tasks of Administration Server
- Configure [Network Agent policy settings](#)
- Create [installation packages of applications](#)
- Create [virtual Servers](#)
- Assign and configure [distribution points](#)
- Configure [device moving rules](#)
- Configure [rules for auto-tagging devices](#)
- Create [application categories](#)

## 5 Move the imported managed devices under management of Kaspersky Security Center Linux

To complete the migration, move the imported managed devices under management of Kaspersky Security Center Linux. In the current version of Kaspersky Security Center Linux, you can do it by one of the following methods:

- Through the [klmover utility](#).

Use the klmover utility and specify the connection settings for the new Administration Server.

- Through installation or re-installation of Network Agent on the managed devices

Create a new Network Agent installation package and specify the connection settings for the new Administration Server in the installation package properties. Use the installation package to install Network Agent on the imported managed devices through a [remote installation task](#). For more information, see [Switching managed devices under management of Kaspersky Security Center Linux](#).

You can also create and use a [stand-alone installation package](#) to install Network Agent locally.

## 6 Update Network Agent to the latest version

We recommend that you [upgrade the Network Agent for Linux](#) to the same version as Kaspersky Security Center.

## 7 Make sure the managed devices are visible on the new Administration Server

On Kaspersky Security Center Linux Administration Server, open the managed devices list (**Assets (Devices)** → **Managed devices**), and check the values in the **Visible**, **Network Agent is installed**, and **Last connected to Administration Server** columns.

## Other methods of data migration

Besides the Migration wizard, there are other methods to transfer your current objects, but these methods allow you to transfer only policies and tasks:

- [Export the tasks](#) from Kaspersky Security Center Windows, and then [import the tasks](#) to Kaspersky Security Center Linux.

- [Export specific policies](#) from Kaspersky Security Center Windows, and then [import the policies](#) to Kaspersky Security Center Linux. The related policy profiles are exported and imported together with the selected policies.

## Exporting group objects from Kaspersky Security Center Windows

Migration administration group structure, included managed devices and other group objects from Kaspersky Security Center Windows to Kaspersky Security Center Linux requires that you first select data for exporting and create an export file. The export file contains information about all group objects that you want to migrate. The export file will be used for subsequent import to Kaspersky Security Center Linux.

You can export the following objects:

- Tasks and policies of managed applications
- [Global tasks](#)
- Custom device selections
- Administration group structure and included devices
- [Tags](#) that have been assigned to migrating devices

Before you start exporting, read general information about migration to Kaspersky Security Center Linux. Choose the migration method—by using or not using the hierarchy of Administration Servers of Kaspersky Security Center Windows and Kaspersky Security Center Linux.

*To export managed devices and related group objects through the Migration wizard:*

1. Depending on whether or not the Administration Servers of Kaspersky Security Center Windows and Kaspersky Security Center Linux are arranged into a hierarchy, do one of the following:
  - If the Servers are arranged into a hierarchy, open Kaspersky Security Center Web Console, and then switch to the Server of Kaspersky Security Center Windows.
  - If the Servers are not arranged into a hierarchy, open Kaspersky Security Center Web Console connected to Kaspersky Security Center Windows.
2. In the main menu, go to **Operations** → **Migration**.
3. Select **Migrate to Kaspersky Security Center Linux or Kaspersky Single Management Platform** to start the wizard and follow its steps.
4. Select the administration group or subgroup to export. Please make sure that the selected administration group or subgroup contains no more than 10,000 devices.
5. Select the managed applications whose tasks and policies will be exported. Select only applications that are supported by Kaspersky Security Center Linux. The objects of unsupported applications will still be exported, but they will not be operable.
6. Use the links on the left to select the global tasks, device selections, and reports to export. The **Group objects** link allows you to exclude custom roles, internal users and security groups, and custom application categories from the export.

The export file (ZIP archive) is created. Depending on whether or not you perform migration with Administration Server hierarchy support, the export file is saved as follows:

- If the Servers are arranged into a hierarchy, the export file is saved to the temporary folder on Kaspersky Security Center Web Console Server.
- If the Servers are not arranged into a hierarchy, the export file is downloaded to your device.

For migration with Administration Server hierarchy support, [the import starts automatically](#), after a successful export. For migration without Administration Server hierarchy support, you can [import the saved export file to Kaspersky Security Center Linux manually](#).

## Importing the export file to Kaspersky Security Center Linux

To transfer information about managed devices, objects, and their settings that you [exported from Kaspersky Security Center Windows](#), you must import it to Kaspersky Security Center Linux or Kaspersky XDR Expert.

*To import managed devices and related group objects through the Migration wizard:*

1. Depending on whether or not the Administration Servers of Kaspersky Security Center Windows and Kaspersky Security Center Linux are arranged into a hierarchy, do one of the following:
  - If the Servers are arranged into a hierarchy, proceed to the next step of the Migration wizard after the export is completed. The import starts automatically after a [successful export](#) within this wizard (see step 2 of this instruction).
  - If the Servers are not arranged into a hierarchy:
    - a. Open Kaspersky Security Center Web Console connected to Kaspersky Security Center Linux or Kaspersky XDR Expert.
    - b. In the main menu, go to **Operations** → **Migration**.
    - c. Select the export file (ZIP archive) that you created and downloaded during the [export from Kaspersky Security Center Windows](#). The upload of the export file starts.
2. After the export file is uploaded successfully, you can continue importing. If you want to specify another export file, click the **Change** link, and then select the required file.
3. The entire hierarchy of administration groups of Kaspersky Security Center Linux is displayed.  
Select the check box next to the target administration group to which the objects of the exported administration group (managed devices, policies, tasks, and other group objects) must be restored.
4. The import of group objects starts. You cannot minimize the Migration wizard and perform any concurrent operations during the import. Wait until the refresh icons (↻) next to all items in the list of objects are replaced with green check marks (✓) and the import finishes.
5. When the import completes, the exported structure of administration groups, including device details, appears under the target administration group that you selected. If the name of the object that you restore is identical to the name of an existing object, the restored object has an incremental suffix added.

If in a migrated task the [details of the account under which the task is run are specified](#), you have to open the task and enter the password again after the import is completed.

If the import has completed with an error, you can do one of the following:

- For migration with Administration Server hierarchy support, you can start to import the export file again.
- For migration without Administration Server hierarchy support, you can start the Migration wizard to select another export file, and then import it again.

You can check whether the group objects included in the export scope have been successfully imported to Kaspersky Security Center Linux. To do this, go to the **Assets (Devices)** section and ensure whether the imported objects appear in the corresponding subsections.

Note that the imported managed devices are displayed in the **Managed devices** subsection, but they are invisible in the network and Network Agent is not installed and running on them (the *No* value in the **Visible**, **Network Agent is installed**, and **Network Agent is running** columns).

To complete the migration, you need to [switch the managed devices to be under management of Kaspersky Security Center Linux](#).

## Switching managed devices to be under management of Kaspersky Security Center Linux

After a successful import of information about managed devices, objects, and their settings to Kaspersky Security Center Linux, you need to switch the managed devices to be under management of Kaspersky Security Center Linux to complete the migration.

In the current version of Kaspersky Security Center Linux, you can move the managed devices to be under Kaspersky Security Center Linux either by using the [klmover utility](#), or by installing Network Agent on the managed devices through a [remote installation task](#).

*To switch managed devices to be under management of Kaspersky Security Center Linux by installing Network Agent:*

1. Switch to Administration Server of Kaspersky Security Center Windows.
2. Go to **Discovery & deployment** → **Deployment & assignment** → **Installation packages**, and then open the [properties](#) of an existing installation package of Network Agent.  
If the installation package of Network Agent is absent in the package list, [download a new one](#).
3. On the **Settings** tab, select the **Connection** section. Specify the connection settings of Administration Server of Kaspersky Security Center Linux.
4. Create a [remote installation task](#) for imported managed devices, and then specify the reconfigured Network Agent installation package.

You can install Network Agent through Administration Server of Kaspersky Security Center Windows or through a Windows-based device that acts as [a distribution point](#). If you use Administration Server, enable the **Using operating system resources through Administration Server** option. If you use a distribution point, enable the **Using operating system resources through distribution points** option.

5. Run the remote installation task.

After the remote installation task finishes successfully, go to Administration Server of Kaspersky Security Center Linux and ensure that managed devices are visible in the network, and that Network Agent is installed and running on them (the *Yes* value in the **Visible**, **Network Agent is installed**, and **Network Agent is running** columns).

## Configuring Administration Server

This section describes the configuration process and properties of Kaspersky Security Center Administration Server.

## Configuring the connection of Kaspersky Security Center Web Console to Administration Server

*To set the connection ports of Administration Server:*

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 **Connection ports** section.

The application displays the main connection settings of the selected server.

## Configuring an allowlist of IP addresses to log in to Kaspersky Security Center Linux

By default, users can log in to Kaspersky Security Center Linux under any device where they can open Kaspersky Security Center Web Console. However, you can configure Administration Server so that users can connect to it only from devices with allowed IP addresses. In this case, even if an intruder steals a Kaspersky Security Center Linux account, he or she will not be able to log in to Kaspersky Security Center Linux because the IP address of the intruder's device is not in the allowlist.

The IP address is verified when a user logs in to Kaspersky Security Center Linux or runs an [application](#) that interacts with Administration Server via [Kaspersky Security Center Linux OpenAPI](#). At this moment, a user's device tries to establish a connection with Administration Server. If the IP address of the device is not in the allowlist, an authentication error occurs and the [KLAUD\\_EV\\_SERVERCONNECT event](#) notifies you that a connection with Administration Server has not been established.

### Requirements for an allowlist of IP addresses

IP addresses are verified only when the following applications try to connect to Administration Server:

- Kaspersky Security Center Web Console Server

If you sign in to Kaspersky Security Center Linux through Kaspersky Security Center Web Console, you can configure a firewall on the device where Kaspersky Security Center Web Console Server is installed using the standard means of operating system. Then, if someone tries to log in to Kaspersky Security Center Linux on one device and Kaspersky Security Center Web Console Server is [installed on another device](#), a firewall helps prevent intruders from interfering.

- Applications interacting with Administration Server via klakaut automation objects
- Applications interacting with Administration Server via OpenAPI, such as Kaspersky Anti Targeted Attack Platform or Kaspersky Security for Virtualization

Therefore, specify addresses of the devices on which the applications listed above are installed.

You can set IPv4 and IPv6 addresses. You cannot specify ranges of IP addresses.

## How to establish an allowlist of IP addresses

If you have not set an allowlist earlier, follow the instructions below.

*To establish an allowlist of IP addresses to log in to Kaspersky Security Center Linux:*

1. On the Administration Server device, run the command prompt under an account with administrator rights.
2. Change your current directory to the Kaspersky Security Center Linux installation folder (usually, /opt/kaspersky/ksc64/sbin).

3. Enter the following command under the root account:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "< IP addresses>" -t s
```

Specify IP addresses that meet the requirements listed above. Several IP addresses must be separated by a semicolon.

Example of how to allow only one device to connect to Administration Server:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s
```

Example of how to allow multiple devices to connect to Administration Server:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
```

4. Restart the Administration Server service.

You can find out whether you have successfully configured the allowlist of IP addresses in the Syslog Event Log on the Administration Server.

## How to change an allowlist of IP addresses

You can change an allowlist just as you did when you first established it. For this purpose, run the same command and specify a new allowlist:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "< IP addresses>" -t s
```

If you want to delete some IP addresses from the allowlist, rewrite it. For example, your allowlist includes the following IP addresses: 192.0.2.0; 198.51.100.0; 203.0.113.0. You want to delete the 198.51.100.0 IP address. To do this, enter the following command at the command prompt:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Do not forget to restart the Administration Server service.

## How to reset a configured allowlist of IP addresses



To reset an already configured allowlist of IP addresses:

1. Enter the following command at the command prompt under the root account:  
`k1scflag -fset -pv k1server -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. Restart the Administration Server service.

After that, IP addresses are not verified any more.

## Configuring internet access settings for Administration Server

You must configure internet access to use Kaspersky Security Network, and to download updates of anti-virus databases for Kaspersky Security Center Linux and managed Kaspersky applications.

To specify the internet access settings for Administration Server:

1. In the main menu, click the settings icon (⚙️) next to the Administration Server name.  
The Administration Server properties window opens.
2. On the **General** tab, select the **Configuring internet access** section.
3. Enable the **Use proxy server** option if you want to use a proxy server when connecting to the internet. If this option is enabled, the fields are available for entering settings. Specify the following settings for a proxy server connection:

- **Address** [?](#)

Address of the proxy server used for Kaspersky Security Center Linux connection to the internet.

- **Port number** [?](#)

Number of the port through which Kaspersky Security Center Linux proxy connection will be established.

- **Bypass proxy server for local addresses** [?](#)

No proxy server will be used to connect to devices in the local network.

- **Proxy server authentication** [?](#)

If this check box is selected, in the entry fields you can specify the credentials for proxy server authentication.

This entry field is available if the **Use proxy server** check box is selected.

- **User name** [?](#)

User account under which connection to the proxy server is established (this field is available if the **Proxy server authentication** check box is selected).

- [Password](#) 

Password set by the user under whose account the proxy server connection is established (this field is available if the **Proxy server authentication** check box is selected).

To see the entered password, click and hold the **Show** button for as long as you require.

You can also configure internet access by using the [quick start wizard](#).

## Hierarchy of Administration Servers

Some client companies, for example MSP, may run multiple Administration Servers. It can be inconvenient to administer several separate Administration Servers, so a hierarchy can be applied. In a hierarchy, a Linux-based Administration Server can work both as a primary Server and as a secondary Server. The primary Linux-based Server can manage both Linux-based and Windows-based secondary Servers. A primary Windows-based Server can manage a secondary Linux-based Server.

A "primary/secondary" configuration for two Administration Servers provides the following options:

- A secondary Administration Server inherits policies, tasks, user roles, and installation packages from the primary Administration Server, thus preventing duplication of settings.
- Selections of devices on the primary Administration Server can include devices from secondary Administration Servers.
- Reports on the primary Administration Server can contain data (including detailed information) from secondary Administration Servers.
- A primary Administration Server can be used as a source of updates for a secondary Administration Server.

The primary Administration Server only receives data from non-virtual secondary Administration Servers within the scope of the options listed above. This limitation does not apply to virtual Administration Servers, which share the database with their primary Administration Server.

## Creating a hierarchy of Administration Servers: adding a secondary Administration Server

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

### Adding secondary Administration Server (performed on the future primary Administration Server)

You can add an Administration Server as a secondary Administration Server, thus establishing a "primary/secondary" hierarchy.

*To add a secondary Administration Server that is available for connection through Kaspersky Security Center Web Console:*

1. Make sure that port 13000 of the future primary Administration Server is available for receipt of connections from secondary Administration Servers.

2. On the future primary Administration Server, click the settings icon (⚙️).
3. On the properties page that opens, click the **Administration Servers** tab.
4. Select the check box next to the name of the administration group to which you want to add the Administration Server.
5. In the menu line, click **Connect secondary Administration Server**.  
The Add secondary Administration Server wizard starts.
6. On the first page of the wizard, 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.

- [Administration Server SSL port](#) ⓘ

Specify the number of the SSL port on the primary Administration Server. The default port number is 13000.

- [Administration Server API port](#) ⓘ

Specify the number of the port on the primary Administration Server for receiving connections over OpenAPI. The default port number is 13299.

- [Connect primary Administration Server to secondary Administration Server in DMZ](#) ⓘ

Select this option if the secondary Administration Server is in a demilitarized zone (DMZ).  
If this option is selected, the primary Administration Server initiates connection to the secondary Administration Server. Otherwise, the secondary Administration Server initiates connection to the primary Administration Server.

- [Use proxy server](#) ⓘ

Select this option if you use a proxy server to connect to the secondary Administration Server.

In this case, you also have to specify the following settings of the proxy server:

- **Address**
- **User name**
- **Password**

7. Specify the connection settings:

- Enter the address of the future primary Administration Server.
- If the future secondary Administration Server uses a proxy server, enter the proxy server address and user credentials to connect to the proxy server.

8. Enter the credentials of the user that has access rights on the future secondary Administration Server.

Make sure that two-step verification is disabled for the account that you specify. If two-step verification is enabled for this account, then you can create the hierarchy from the future secondary Server only (see instructions below). This is a [known issue](#).

If the connection settings are correct, the connection with the future secondary Server is established and the "primary/secondary" hierarchy is built. If the connection has failed, check the connection settings or specify the certificate of the future secondary Server manually.

The connection may also fail because the future secondary Server is authenticated with a self-signed certificate that was automatically generated by Kaspersky Security Center Linux. As a result, the browser might block downloading the self-signed certificate. If this is the case, you can do one of the following:

- For the future secondary Server, create a certificate that is trusted in your infrastructure and that meets the [requirements for custom certificates](#).
- Add the self-signed certificate of the future secondary Server to the list of trusted browser certificates. We recommend that you use this option only if you cannot create a custom certificate. For the information about adding a certificate to the list of trusted certificates, refer to the documentation of your browser.

After the wizard finishes, the "primary/secondary" hierarchy is built. Connection between the primary and secondary Administration Servers is established through port 13000. The tasks and policies from the primary Administration Server are received and applied. The secondary Administration Server is displayed on the primary Administration Server, in the administration group to which it was added.


## Adding secondary Administration Server (performed on the future secondary Administration Server)

If you could not connect to the future secondary Administration Server (for example, because it was temporarily disconnected or unavailable or because the certificate file of secondary Administration Server is self-signed), you are still able to add a secondary Administration Server.

*To add as secondary an Administration Server that is not available for connection through Kaspersky Security Center Web Console:*

1. Send the certificate file of the future primary Administration Server to the system administrator of the office where the future secondary Administration Server is located. (You can, for example, write the file to an external device, such as a flash drive, or send it by email.)


The certificate file is located on the future primary Administration Server, at `/var/opt/kaspersky/klnagent_srv/1093/cert/`.

2. Prompt the system administrator in charge of the future secondary Administration Server to do the following:
  - a. Click the settings icon .
  - b. On the properties page that opens, proceed to the **Hierarchy of Administration Servers** section of the **General** tab.
  - c. Select the **This Administration Server is secondary in the hierarchy** option.
  - d. In the **Primary Administration Server address** field, enter the network name of the future primary Administration Server.
  - e. Select the previously saved file with the certificate of the future primary Administration Server by clicking **Browse**.
  - f. If necessary, select the **Connect primary Administration Server to secondary Administration Server in DMZ** check box.
  - g. If the connection to the future primary Administration Server is performed through a proxy server, select the **Use proxy server** option and specify the connection settings.
  - h. Click **Save**.

The "primary/secondary" hierarchy is built. The primary Administration Server starts receiving connection from the secondary Administration Server using port 13000. The tasks and policies from the primary Administration Server are received and applied. The secondary Administration Server is displayed on the primary Administration Server, in the administration group where it was added.

## Viewing the list of secondary Administration Servers

*To view the list of the secondary (including virtual) Administration Servers:*


In the main menu, click the name of the Administration Server, which is next to the settings icon .

The drop-down list of the secondary (including virtual) Administration Servers is displayed.

You can proceed to any of these Administration Servers by clicking its name.

The administration groups are shown, too, but they are grayed and not available for management in this menu.

If you are connected to your primary Administration Server in Kaspersky Security Center Web Console, and can not connect to a virtual Administration Server that is managed by a secondary Administration Server, you can use one of the following ways:

- [Modify the existing Kaspersky Security Center Web Console installation to add the secondary Server to the list of trusted Administration Servers](#) . Then you will be able to connect to the virtual Administration Server in Kaspersky Security Center Web Console.

1. On the device where Kaspersky Security Center Web Console is installed, run the Kaspersky Security Center Web Console installation file corresponding to the Linux distribution installed on your device under an account with administrative privileges.
2. The Setup Wizard will start.
3. On the first page of the Wizard, select the **Upgrade** option.
4. On the **Modification type** page, select the **Edit connection settings** option.
5. On the **Trusted Administration Servers** page, add the required secondary Administration Server.
6. On the last page of the Wizard, click **Modify** to apply the new settings.
7. After the application reconfiguration successfully completes, click the **Finish** button.

- Use Kaspersky Security Center Web Console to [connect directly to the secondary Administration Server](#) where the virtual Server was created. Then you will be able to switch to the virtual Administration Server in Kaspersky Security Center Web Console.

## Managing virtual Administration Servers


This section describes the following actions to manage virtual Administration Servers:

- [Create virtual Administration Servers](#)
- [Enable and disable virtual Administration Servers](#)
- [Assign an administrator for a virtual Administration Server](#)
- [Change the Administration Server for client devices](#)
- [Delete virtual Administration Servers](#)

## Creating a virtual Administration Server

You can create [virtual Administration Servers](#) and add them to administration groups.

*To create and add a virtual Administration Server:*

1. In the main menu, click the settings icon  next to the name of the required Administration Server.
2. On the page that opens, proceed to the **Administration Servers** tab.

3. Select the administration group to which you want to add a virtual Administration Server.  
The virtual Administration Server will manage devices from the selected group (including the subgroups).

4. On the menu line, click **New virtual Administration Server**.

5. On the page that opens, define the properties of the new virtual Administration Server:

- **Name of virtual Administration Server.**
- **Administration Server connection address**


You can specify the name or the IP address of your Administration Server.

6. From the list of users, select the virtual Administration Server administrator. If you want, you can edit one of the existing accounts before assigning it the administrator's role, or create a new user account.

7. Click **Save**.

The new virtual Administration Server is created, added to the administration group and displayed on the **Administration Servers** tab.

If you are connected to your primary Administration Server in Kaspersky Security Center Web Console, and can not connect to a virtual Administration Server that is managed by a secondary Administration Server, you can use one of the following ways:

- [Modify the existing Kaspersky Security Center Web Console installation to add the secondary Server to the list of trusted Administration Servers](#) . Then you will be able to connect to the virtual Administration Server in Kaspersky Security Center Web Console.

1. On the device where Kaspersky Security Center Web Console is installed, run the Kaspersky Security Center Web Console installation file corresponding to the Linux distribution installed on your device under an account with administrative privileges.

2. The Setup Wizard will start.

3. On the first page of the Wizard, select the **Upgrade** option.

4. On the **Modification type** page, select the **Edit connection settings** option.

5. On the **Trusted Administration Servers** page, add the required secondary Administration Server.

6. On the last page of the Wizard, click **Modify** to apply the new settings.

7. After the application reconfiguration successfully completes, click the **Finish** button.

- Use Kaspersky Security Center Web Console to [connect directly to the secondary Administration Server](#) where the virtual Server was created. Then you will be able to switch to the virtual Administration Server in Kaspersky Security Center Web Console.

## Enabling and disabling a virtual Administration Server

When you create a new virtual Administration Server, it is enabled by default. You can disable or enable it again at any time. Disabling or enabling a virtual Administration Server is equal to switching off or on a physical Administration Server.

*To enable or disable a virtual Administration Server:*

1. In the main menu, click the settings icon (⚙️) next to the name of the required Administration Server.
2. On the page that opens, proceed to the **Administration Servers** tab.
3. Select the virtual Administration Server that you want to enable or disable.
4. On the menu line, click the **Enable / disable virtual Administration Server** button.

The virtual Administration Server state is changed to enabled or disabled, depending on its previous state. The updated state is displayed next to the Administration Server name.

## Assigning an administrator for a virtual Administration Server

When you use virtual Administration Servers in your organization, you might want to assign a dedicated administrator for each virtual Administration Server. For example, this might be useful when you create virtual Administration Servers to manage separate offices or departments of your organization, or if you are an MSP provider and you manage your tenants through virtual Administration Servers.

When you create a virtual Administration Server, it inherits the user list and all of the user rights of the primary Administration Server. If a user has access rights to the primary Server, this user has access rights to the virtual Server as well. After creation, you configure the access rights to the Servers independently. If you want to assign an administrator for a virtual Administration Server only, make sure that the administrator does not have access rights on the primary Administration Server.

You assign an administrator for a virtual Administration Server by granting the administrator access rights to the virtual Administration Server. You can grant the required access rights in one of the following ways:

- Configure access rights for the administrator manually
- Assign one or more user roles for the administrator

To [sign in to Kaspersky Security Center Web Console](#), an administrator of a virtual Administration Server specifies the virtual Administration Server name, user name, and password. Kaspersky Security Center Web Console authenticates the administrator and opens the virtual Administration Servers to which the administrator has access rights. The administrator cannot switch between Administration Servers.

### Prerequisites

Before you start, ensure that the following conditions are met:

- The [virtual Administration Server is created](#).
- On the primary Administration Server, you have created an account for the administrator that you want to assign for the virtual Administration Server.
- You have the [Modify object ACLs](#) right in the **General features** → **User permissions** functional area.



## Configuring access rights manually

*To assign an administrator for a virtual Administration Server:*

1. In the main menu, switch to the required virtual Administration Server:
    - a. Click the chevron icon (▾) to the right of the current Administration Server name.
    - b. Select the required Administration Server.
  2. In the main menu, click the settings icon (⚙) next to the name of the Administration Server.  
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.

## 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. In the main menu, switch to the required virtual Administration Server:
  - a. Click the chevron icon (▾) to the right of the current Administration Server name.
  - b. Select the required Administration Server.
3. [Assign the new role or several roles to the administrator account.](#)

The application assigns the roles to the administrator account.

## Configuring access rights at the object level

In addition to assigning [access rights at the functional area level](#), you can [configure access to specific objects](#) on the virtual Administration Server, for example, to a specific administration group or a task. To do this, switch to the virtual Administration Server, and then configure the access rights in the object's properties.

## Changing the Administration Server for client devices

You can change the Administration Server that manages client devices to a different Server using the **Change Administration Server** task. After the task completion, the selected client devices will be put under the management of the Administration Server that you specify. You 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 **Assets (Devices) → Tasks**.

2. Click **Add**.

The New task wizard starts. Proceed through the wizard by using the **Next** button.

3. For the Kaspersky Security Center application, select the **Change Administration Server** 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 devices to which the task will be assigned.

6. Select the Administration Server that you want to use to manage the selected devices.

7. 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 on the **Finish task creation** page 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 modify 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 complete, the client devices for which it was created are put under the management of the Administration Server specified in the task settings.

## Deleting a virtual Administration Server

When you delete a virtual Administration Server, all of the objects created on the Administration Server, including policies and tasks, will be deleted as well. The managed devices from the administration groups that were managed by the virtual Administration Server will be removed from the administration groups. To return the devices under management of Kaspersky Security Center Linux, run the network polling, and then move the found devices from the Unassigned devices group to the administration groups.

*To delete a virtual Administration Server:*

1. In the main menu, click the settings icon () next to the name of 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.

## Viewing log of connections to the Administration Server

The history of connections and attempts to connect to the Administration Server during its operation can be saved to a log file. The information in the file allows you to track not only connections inside your network infrastructure, but unauthorized attempts to access the server as well.

*To log events of connection to the Administration Server:*

1. In the main menu, click the settings icon (⚙️) next to the name of the required Administration Server.  
The Administration Server properties window opens.
2. On the **General** tab, select the **Connection ports** section.
3. Enable the **Log Administration Server connection events** option.

All further events of inbound connections to the Administration Server, authentication results, and SSL errors will be saved to the file `/var/opt/kaspersky/klagent_srv/logs/sc.syslog`.

## Setting the maximum number of events in the event repository

In the **Events repository** section of the Administration Server properties window, you can edit the settings of events storage in the Administration Server database by limiting the number of event records and record storage term. When you specify the maximum number of events, the application calculates an approximate amount of storage space required for the specified number. You can use this approximate calculation to evaluate whether you have enough free space on the disk to avoid database overflow. The default capacity of the Administration Server database is 400,000 events. The maximum recommended capacity of the database is 45 million events.

The application checks the database every 10 minutes. If the number of events reaches the specified maximum value plus 10,000, the application deletes the oldest events so that only the specified maximum number of events remains.

When the Administration Server deletes old events, it cannot save new events to the database. During this period of time, information about events that were rejected is written to the operating system log. The new events are queued and then saved to the database after the deletion operation is complete.

*To limit the number of events that can be stored in the events repository on the Administration Server:*

1. In the main menu, click the settings icon (⚙️) next to the name of the required Administration Server.  
The Administration Server properties window opens.
2. On the **General** tab, select the **Events repository** section. Specify the maximum number of events stored in the database.
3. Click the **Save** button.

## Moving Administration Server to another device

If you need to use Administration Server on a new device, you can move it in one of the following ways:

- Move Administration Server and the database server to a new device.
- Keep the database server on the previous device and move only Administration Server to a new device.

*To move Administration Server and the database server to a new device:*

1. On the previous device, create a backup of Administration Server data.

To do this, you can run the [data backup task](#) through Kaspersky Security Center Web Console or run the [klbackup utility](#).

2. Select a new device on which to install the Administration Server. Make sure that the hardware and software on the selected device meet the [requirements](#) for Administration Server, Kaspersky Security Center Web Console, and Network Agent. Also, check that [ports used on Administration Server](#) are available.

3. On the new device, [install the DBMS](#) that the Administration Server will use.

When you select a DBMS, consider the number of devices covered by the Administration Server.

4. Install the Administration Server on the new device.

Note that if you move the database server to the new device, specify the local address as the IP address of the device on which the database is installed (the "h" item in the [Installing Kaspersky Security Center Linux](#) instruction). If you need to keep the database server on the previous device, enter the IP address of the previous device in the "h" item of the [Installing Kaspersky Security Center Linux](#) instruction.

5. After the installation is complete, recover Administration Server data on the new device by using the klbackup utility.

If you use SQL Server as a DBMS on the previous and new devices, note that the version of SQL Server installed on the new device must be the same or later than the version of SQL Server installed on the previous device. Otherwise, you cannot recover Administration Server data on the new device.

6. Open Kaspersky Security Center Web Console and [connect to the Administration Server](#).

7. Verify that all the client devices are connected to the Administration Server.

8. Uninstall the Administration Server and the database server from the previous device.

## Changing DBMS credentials

Sometimes, you may need to change DBMS credentials, for example, in order to perform a credential rotation for security purposes.

*To change DBMS credentials in a Linux environment by using the klsrvconfig utility:*

1. Launch a Linux command line.

2. Specify the klsrvconfig utility in the opened command line window:

```
sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
```

3. Specify a new account name. You should specify credentials of an account that exists in the DBMS.

4. Enter a new password.

5. Specify the new password for confirmation.

The DBMS credentials are changed.

## Backup copying and restoration of Administration Server data

Data backup allows you to move Administration Server from one device to another without data loss. Through backup, you can restore data when moving the Administration Server database to another device, or when upgrading to a newer version of Kaspersky Security Center Linux (moving the Administration Server data to be under management of Kaspersky Security Center Windows is not supported).

Note that the installed management plug-ins are not backed up. After you restore Administration Server data from a backup copy, you need to download and reinstall plug-ins for managed applications.

Before you back up the Administration Server data, check whether a virtual Administration Server is added to the administration group. If a virtual Administration Server is added, make sure that [an administrator is assigned](#) to this virtual Administration Server before the backup. You cannot grant the administrator access rights to the virtual Administration Server after the backup. Note that if the administrator account credentials are lost, you will not be able to assign a new administrator to the virtual Administrator Server.

You can create a backup copy of Administration Server data in one of the following ways:

- By creating and running a [data backup task](#) through Kaspersky Security Center Web Console.
- By running the [klbackup utility](#) on the device that has Administration Server installed. This utility is included in the Kaspersky Security Center distribution kit. After the installation of Administration Server, the utility is located in the root of the destination folder specified at the application installation (usually, `/opt/kaspersky/ksc64/sbin/klbackup`).

The following data is saved in the backup copy of Administration Server:

- Database of Administration Server (policies, tasks, application settings, events saved on the Administration Server).
- Configuration details of the structure of administration groups and client devices.
- Repository of distribution packages of applications for remote installation.
- Administration Server certificate.

Recovery of Administration Server data is only possible using the klbackup utility.

## Creating an Administration Server data backup task

Backup tasks are Administration Server tasks; they are created through the [quick start wizard](#). If a backup task created by the quick start wizard has been deleted, you can create one manually.

The *Backup of Administration Server data* task can only be created in a single copy. If the Administration Server data backup task has already been created for the Administration Server, it is not displayed in the task type selection window.

*To create an Administration Server data backup task:*

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

2. Click **Add**.

The New task wizard starts.

3. On the first page of the wizard, in the **Application** list, select **Kaspersky Security Center 15**, and in the **Task type** list, select **Backup of Administration Server data**.

4. On the corresponding page of the wizard, specify the following information:

- Folder for storage of backup copies
- Password for the backup (optional)
- Maximum number of backup copies to save

5. If on the **Finish task creation** page 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 modify the default settings later, at any time.

6. Click the **Finish** button.

The task is created and displayed in the list of tasks.

## Using the kbackup utility to back up and recover data

You can copy Administration Server data for backup and future recovery using the kbackup utility, which is part of the Kaspersky Security Center distribution kit.

*To create a backup copy or recover Administration Server data in silent mode,*

Run kbackup with the required set of keys from the command line of the device that has Administration Server installed.

Utility command line syntax:

```
kbackup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts][[-restore] [-password PASSWORD] [-online]
```

If no password is specified in the command line of the kbackup utility, the utility prompts you to enter the password interactively.

Descriptions of the keys:

- **-path BACKUP\_PATH**—Save information in the BACKUP\_PATH folder, or use data from the BACKUP\_PATH folder for recovery (mandatory parameter).
- **-logfile LOGFILE**—Save a report about Administration Server data backup and recovery.  
The database server account and the kbackup utility should be granted permissions for changing data in the folder BACKUP\_PATH.
- **-use\_ts**—When saving data, copy information to the BACKUP\_PATH folder, to the subfolder with a name containing the current system date and operation time in kbackup YYYY-MM-DD # HH-MM-SS format. If no key is specified, information is saved in the root of the folder BACKUP\_PATH.

During attempts to save information in a folder that already stores a backup copy, an error message appears. No information will be updated.

Availability of the `-use_ts` key allows an Administration Server data archive to be maintained. For example, if the `-path` key indicates the folder `C:\KLBackups`, the folder `klbackup 2022/6/19 # 11-30-18` then stores information about the status of the Administration Server as of June 19, 2022, at 11:30:18 AM.

- `-restore`—Recover Administration Server data. Data recovery is performed based on information contained in the `BACKUP_PATH` folder. If no key is available, data is backed up in the `BACKUP_PATH` folder.
- `-password PASSWORD`—Save or recover the Administration Server certificate; to encrypt and decrypt the certificate, use the password specified by the `PASSWORD` parameter.

A forgotten password cannot be recovered. There are no password requirements. The password length is unlimited and zero length (no password) is also possible.

When restoring data, you must specify the same password that was entered during backup. If the path to a shared folder changed after backup, check the operation of tasks that use restored data (restore tasks and remote installation tasks). If necessary, edit the settings of these tasks. While data is being restored from a backup file, no one must access the shared folder of Administration Server. The account under which the `klbackup` utility is started must have full access to the shared folder. We recommend that you run the utility on a newly installed Administration Server.

- `-online`—Back up Administration Server data by creating a volume snapshot to minimize the offline time of the Administration Server. When you use the utility to recover data, this option is ignored.

## Administration Server maintenance

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

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

- Checks the database for errors.
- Re-organizes database indexes.
- Updates the database statistics.
- Shrinks the database (if necessary).

The Administration Server maintenance task supports MariaDB versions 10.3 and later. If you use MariaDB versions 10.2 or earlier, administrators have to maintain this DBMS on their own.

The Administration Server maintenance task is created automatically when you install Kaspersky Security Center Linux. If the Administration Server maintenance task is deleted, you can create it manually.

*To create the Administration Server maintenance task:*

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



2. Click the **Add** button.

The New task wizard starts.

3. In the **New task** window of the wizard, select **Administration Server maintenance** as the task type and click the **Next** button.

4. Follow the rest of the wizard instructions.

The newly created task is displayed in the list of tasks. Only one Administration Server maintenance task can be running for a single Administration Server. If an Administration Server maintenance task has already been created for an Administration Server, no new Administration Server maintenance task can be created.

## Deleting a hierarchy of Administration Servers

If you no longer want to have a hierarchy of Administration Servers, you can disconnect them from this hierarchy.

*To delete a hierarchy of Administration Servers:*

1. In the main menu, click the settings icon (⚙️) next to 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.

## Access to public DNS servers

If access to Kaspersky servers by using the system DNS is not possible, Kaspersky Security Center Linux can use the following public DNS servers, in the following order:

1. Google Public DNS (8.8.8.8)

2. Cloudflare DNS (1.1.1.1)

3. Alibaba Cloud DNS (223.6.6.6)

4. Quad9 DNS (9.9.9.9)

5. CleanBrowsing (185.228.168.168)

Requests to these DNS servers may contain domain addresses and the public IP address of the Administration Server, because the application establishes a TCP/UDP connection to the DNS server. If Kaspersky Security Center Linux is using a public DNS server, data processing is governed by the privacy policy of the relevant service.

*To configure the use of public DNS by using the `klscflag` utility:*

1. Run the command line, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.
2. To disable the use of public DNS, run the following command under the root account:  

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
```
3. To enable the use of public DNS, run the following command under the root account:  

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
```

## Configuring the interface

You can configure the Kaspersky Security Center Web Console interface to display and hide sections and interface elements, depending on the features being used.

*To configure the Kaspersky Security Center Web Console interface in accordance with the currently used set of features:*

1. In the main menu, go to your account settings, and then select **Interface options**.
2. In the **Interface options** window that opens, enable or disable the **Show data encryption and protection** option.
3. Click **Save**.

After that, the **Operations** → **Data encryption and protection** section appears in the main menu.

## Encrypt communication with TLS

To fix vulnerabilities on your organization's corporate network, you can enable traffic encryption by using the TLS protocol. You can enable TLS encryption protocols and supported cipher suites on Administration Server. Kaspersky Security Center Linux supports the TLS protocol versions 1.0, 1.1, 1.2, and 1.3. You can select the required encryption protocol and cipher suites.

Kaspersky Security Center Linux uses self-signed certificates. You can also use your own certificates. Kaspersky specialists recommend using certificates issued by trusted certificate authorities.

*To configure allowed encryption protocols and cipher suites on Administration Server:*

1. Run the command line, and then change your current directory to the directory with the klscflag utility. The klscflag utility is located in the directory where the Administration Server is installed. The default installation path is /opt/kaspersky/ksc64/sbin.
2. Use the SrvUseStrictSslSettings flag to configure allowed encryption protocols and cipher suites on Administration Server. Execute the following command in the command line under the root account:  

```
klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <value> -t d
```

Specify the <value> parameter of the SrvUseStrictSslSettings flag:

- 4—Only the TLS 1.2 and TLS 1.3 protocols are enabled. Also, cipher suites with TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 are enabled (these cipher suites are needed for backward

compatibility with Kaspersky Security Center 11). This is the default value.

Cipher suites supported for the TLS 1.2 protocol:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- AES256-GCM-SHA384 (cipher suite with TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384)
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Cipher suites supported for the TLS 1.3 protocol:

- TLS\_AES\_256\_GCM\_SHA384
  - TLS\_CHACHA20\_POLY1305\_SHA256
  - TLS\_AES\_128\_GCM\_SHA256
  - TLS\_AES\_128\_CCM\_SHA256
- 5—Only the TLS 1.2 and TLS 1.3 protocols are enabled. For the TLS 1.2 and TLS 1.3 protocols, the specific cipher suites listed below are supported.

Cipher suites supported for the TLS 1.2 protocol:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Cipher suites supported for the TLS 1.3 protocol:

- TLS\_AES\_256\_GCM\_SHA384
- TLS\_CHACHA20\_POLY1305\_SHA256
- TLS\_AES\_128\_GCM\_SHA256
- TLS\_AES\_128\_CCM\_SHA256

We do not recommend using 0, 1, 2, or 3 as the parameter value of the SrvUseStrictSslSettings flag. These parameter values correspond to insecure TLS protocol versions (TLS 1.0 and TLS 1.1) and insecure cipher suites, and are used only for backward compatibility with earlier Kaspersky Security Center versions.

3. Restart the following Kaspersky Security Center Linux services:

- Administration Server
- Web Server
- Activation Proxy

As a result, traffic encryption by using the TLS protocol is enabled.

You can use the `KLTR_TLS12_ENABLED` and `KLTR_TLS13_ENABLED` flags to enable the support of the TLS 1.2 and TLS 1.3 protocols, respectively. These flags are enabled by default.

*To enable or disable the support of the TLS 1.2 and TLS 1.3 protocols:*

1. Run the `klscflag` utility.

Run the command line, and then change your current directory to the directory with the `klscflag` utility. The `klscflag` utility is located in the directory where the Administration Server is installed. The default installation path is `/opt/kaspersky/ksc64/sbin`.

2. Execute one of the following commands in the command line under the root account:

- Use this command to enable or disable the support of the TLS 1.2 protocol:

```
klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <value> -t d
```

- Use this command to enable or disable the support of the TLS 1.3 protocol:

```
klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <value> -t d
```

Specify the `<value>` parameter of the flag:

- 1—To enable the support of the TLS protocol.
- 0—To disable the support of the TLS protocol.

# Discovering networked devices

This section describes search and discovery of networked devices.

Kaspersky Security Center Linux allows you to find devices on the basis of specified criteria. You can save search results to a text file.

The search and discovery feature allows you to find the following devices:

- Managed devices in administration groups of Kaspersky Security Center Administration Server and its secondary Administration Servers.
- Unassigned devices managed by Kaspersky Security Center Administration Server and its secondary Administration Servers.

## Scenario: Discovering networked devices

You must perform device discovery before installation of the security applications. When all networked devices are discovered, you can receive information about them and manage them through policies. Regular network polls are needed to discover if there are any new devices and whether previously discovered devices are still on the network.

Discovery of networked devices proceeds in stages:

### 1 Initial device discovery

When you complete the quick start wizard, perform device discovery manually.

### 2 Configuring future polls

Make sure that [IP range polling](#) is enabled and that the poll schedule meets the needs of your organization. When configuring the poll schedule, use the recommendations for network polling frequency.

You can also enable [Zeroconf polling](#) if your network includes IPv6 devices.

If networked devices are included in a domain, it is recommended to use [domain controller polling](#).

### 3 Setting up rules for adding discovered devices to administration groups (optional)

If new devices appear on your network, they are discovered during regular polls and are automatically included 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 stage, all the newly discovered devices go to the **Unassigned devices** group and stay there. If you want, you can move these devices to the **Managed devices** group manually. If you move the devices to the **Managed devices** group manually, you can analyze information about each device and decide whether you want to move it to an administration group, and, if so, to which group.

## Results

Completion of the scenario yields the following:

- Kaspersky Security Center Linux Administration Server discovers the devices that are on the network and provides you with information about them.
- Future polls are set up and are conducted according to the specified schedule.

The newly discovered devices are arranged according to the configured rules. (Or, if no rules are configured, the devices stay in the **Unassigned devices** group).

## IP range polling

Kaspersky Security Center Linux attempts to perform reverse name resolution for every IPv4 address from the specified range to a DNS name using standard DNS requests. If this operation succeeds, the server sends an ICMP ECHO REQUEST (the same as the ping command) to the received name. If the device responds, the information about it is added to the Kaspersky Security Center Linux database. The reverse name resolution is necessary to exclude the network devices that can have an IP address but are not computers, for example, network printers or routers.

This polling method relies upon a correctly configured local DNS service. It must have a reverse lookup zone. If this zone is not configured, IP subnet polling will yield no results.

Initially, Kaspersky Security Center Linux gets IP ranges for polling from the network settings of the device on which it is installed. If the device address is 192.168.0.1 and the subnet mask is 255.255.255.0, Kaspersky Security Center Linux includes the network 192.168.0.0/24 in the list of polling address automatically. Kaspersky Security Center Linux polls all addresses from 192.168.0.1 to 192.168.0.254.

If only IP range polling is enabled, Kaspersky Security Center Linux discovers devices only with IPv4 addresses. If your network includes IPv6 devices, turn on [Zeroconf polling](#) of devices.

## Viewing and modifying the settings for IP range polling

*To view and modify the properties of IP range polling:*

1. In the main menu, go to **Discovery & deployment** → **Discovery** → **IP ranges**.

2. Click the **Properties** button.

The IP polling properties window opens.

3. Enable or disable IP polling by using the **Allow polling** toggle button.

4. Configure the poll schedule. By default, IP polling runs every 420 minutes (seven hours).

When specifying the polling interval, make sure that this setting does not exceed the value of the [IP address lifetime parameter](#). If an IP address is not verified by polling during the IP address lifetime, this IP address is automatically removed from the polling results. By default, the life span of the polling results is 24 hours, because dynamic IP addresses (assigned using Dynamic Host Configuration Protocol (DHCP)) change every 24 hours.

Polling schedule options:

- [Every N days](#) ⓘ

The polling runs regularly, with the specified interval in days, starting from the specified date and time.  
By default, the polling runs every day, starting from the current system date and time.

- [Every N minutes](#) ⓘ

The polling runs regularly, with the specified interval in minutes, starting from the specified time.

- [By days of week](#) <sup>?</sup>

The polling runs regularly, on the specified days of week, and at the specified time.

- [Every month on specified days of selected weeks](#) <sup>?</sup>

The polling runs regularly, on the specified days of each month, and at the specified time.

- [Run missed tasks](#) <sup>?</sup>

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.

5. Click the **Save** button.

The properties are saved and applied to all IP ranges.

## Running the poll manually

*To run the poll immediately,*

Click **Start poll**.

## Adding and modifying an IP range

Initially, Kaspersky Security Center Linux gets IP ranges for polling from the network settings of the device on which it is installed. If the device address is 192.168.0.1 and the subnet mask is 255.255.255.0, Kaspersky Security Center Linux includes the network 192.168.0.0/24 in the list of polling address automatically. Kaspersky Security Center Linux polls all addresses from 192.168.0.1 to 192.168.0.254. You can modify the automatically defined IP ranges or add custom IP ranges.

You can create a range only for IPv4 addresses. If you enable [Zeroconf polling](#), Kaspersky Security Center Linux will poll the whole network.

*To add a new IP range:*

1. In the main menu, go to **Discovery & deployment** → **Discovery** → **IP ranges**.
2. To add a new IP range, click the **Add** button.
3. In the window that opens, specify the following settings:

- [IP range name](#) <sup>?</sup>

A name of the IP range. You might want to specify the IP range itself as its name, for example, "192.168.0.0/24".

- [IP interval or subnet address and mask](#) 

Set the IP range by specifying either the start and end IP addresses or the subnet address and subnet mask. You can also select one of the already existing IP ranges by clicking the **Browse** button.

- [IP address lifetime \(hours\)](#) 

When specifying this parameter make sure that it exceeds the polling interval set in the [polling schedule](#). If an IP address is not verified by polling during the IP address lifetime, this IP address is automatically removed from the polling results. By default, the life span of the polling results is 24 hours, because dynamic IP addresses (assigned using Dynamic Host Configuration Protocol (DHCP)) change every 24 hours.

4. Select **Enable IP range polling** if you want to poll the subnet or interval that you have added. Otherwise, the subnet or interval that you have added will not be polled.

5. Click the **Save** button.

The new IP range is added to the list of IP ranges.

You can run polling of each IP range separately by using the **Start poll** button. By default, the life span of the polling results is 24 hours and it is equal to the IP address lifetime setting.

*To add a subnet to an existing IP range:*

1. In the main menu, go to **Discovery & deployment** → **Discovery** → **IP ranges**.

2. Click the name of the IP range to which you want to add a subnet.

3. In the window that opens, click the **Add** button.

4. Specify a subnet by using either its address and mask, or by using the first and last IP address in the IP range. Or, add an existing subnet by clicking the **Browse** button.

5. Click the **Save** button.

The new subnet is added to the IP range.

6. Click the **Save** button.

The new settings of the IP range are saved.

You can add as many subnets as you need. Named IP ranges are not allowed to overlap, but unnamed subnets inside an IP range have no such restrictions. You can enable and disable polling independently for every IP range.

## Zeroconf polling



This polling type is supported only for Linux-based distribution points.

Kaspersky Security Center Linux can poll networks that have devices with IPv6 addresses. In this case, IP ranges are not specified and Kaspersky Security Center Linux polls the whole network by using [zero-configuration networking](#) (also referred to as *Zeroconf*). To start using Zeroconf, you must install the avahi-browse utility on the Linux device that polls networks—Administration Server or a distribution point.

*To enable Zeroconf polling:*

1. In the main menu, go to **Discovery & deployment** → **Discovery** → **IP ranges**.
2. Click the **Properties** button.
3. In the opened window, turn on the **Use Zeroconf to poll IPv6 networks** toggle button.

After that, Kaspersky Security Center Linux starts to poll your network. In this case, the specified IP ranges are ignored.

## Domain controller polling

Kaspersky Security Center Linux supports polling of a 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](#).

When you poll a domain controller, Administration Server or a distribution point retrieves information about the domain structure, user accounts, security groups, and DNS names of the devices that are included in the domain.

We recommend using domain controller polling if all networked devices are members of a domain. If some of the networked devices are not included in the domain, these devices cannot be discovered by domain controller polling.

### Prerequisites

Before you poll a domain controller, ensure that 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 Administration Server

*To poll a domain controller by using Administration Server:*

1. In the main menu, go to **Discovery & deployment** → **Discovery** → **Domain controllers**.
2. Click **Polling settings**.

The **Domain controller polling settings** window opens.

3. Select the **Enable domain controller polling** option.
4. In the **Poll specified domains**, click **Add**, and then specify the address and user credentials of the domain controller.
5. If necessary, in the **Domain controller polling settings** window, specify the polling schedule. The default period is one hour. The data received at the next polling completely replaces old data.

The following polling schedule options are available:

- [Every N days](#) ?

The polling runs regularly, with the specified interval in days, starting from the specified date and time. By default, the polling runs every day, starting from the current system date and time.

- [Every N minutes](#) ?

The polling runs regularly, with the specified interval in minutes, starting from the specified time.

- [By days of week](#) ?

The polling runs regularly, on the specified days of week, and at the specified time.

- [Every month on specified days of selected weeks](#) ?

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 is scheduled.

If this option is enabled, the Administration Server starts polling immediately after it is switched on.

If this option is disabled, the Administration Server waits for the next time for which the polling is scheduled.

By default, this option is disabled.

If you change user accounts in a security group of the domain, these changes will be displayed in Kaspersky Security Center Linux an hour after you poll the domain controller.

6. Click **Save** to apply changes.
7. If you want to perform the poll immediately, click the **Start poll** button.

Domain controller polling by using a distribution point

You can also poll a domain controller by using a distribution point. A Windows- or Linux-based managed device can act as a distribution point.

For a Linux distribution point, polling of a Microsoft Active Directory domain controller and a Samba domain controller are 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. Select the **Enable domain controller polling** option.
4. 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**

5. Click the **Set polling schedule** button to specify the polling schedule options if needed.

Polling starts only according to the specified schedule. Manual start of polling is not available.

After the polling is completed, the domain structure will be displayed in the **Domain controllers** section.

If you set up and enabled [device moving rules](#), the newly discovered devices are automatically included in the **Managed devices** group. If no moving rules have been enabled, the newly discovered devices are automatically included in the **Unassigned devices** group.

The discovered user accounts can be used for [domain authentication in Kaspersky Security Center Web Console](#).

## Authentication and connection to a domain controller

On initial connection to the domain controller the Administration Server identifies the connection protocol. This protocol is used for all future connections to the domain controller.

The initial connection to a domain controller proceeds as follows:

1. Administration Server attempts to connect to the domain controller over TLS.  
By default, certificate verification is not required. Set the `KLNAG_LDAP_TLS_REQCERT` flag to 1 to enforce certificate verification.  
By default, the OS-dependent path to the certificate authority (CA) is used to access the certificate chain. Use the `KLNAG_LDAP_SSL_CACERT` flag to specify a custom path.

2. If the TLS connection fails, Administration Server attempts to connect to the domain controller over SASL (DIGEST-MD5).
3. If the SASL (DIGEST-MD5) connection fails, Administration Server uses Simple Authentication over non-encrypted TCP connection to connect to the domain controller.

You can use the `klscflag` utility to configure flags.

Run the command line, and then change your current directory to the directory with the `klscflag` utility. The `klscflag` utility is located in the directory where the Administration Server is installed. The default installation path is `/opt/kaspersky/ksc64/sbin`.

For example, the following command enforces certificate verification:

```
klscflag -fset -pv klserver -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

## Configuring a Samba domain controller

Kaspersky Security Center Linux supports a Linux domain controller running only on Samba 4.

A Samba domain controller supports the same schema extensions as a Microsoft Active Directory domain controller. You can enable full compatibility of a Samba domain controller with a Microsoft Active Directory domain controller by using the Samba 4 schema extension. This is an optional action.

We recommend enabling full compatibility of a Samba domain controller with a Microsoft Active Directory domain controller. This will ensure the correct interaction between Kaspersky Security Center Linux and the Samba domain controller.

*To enable full compatibility of a Samba domain controller with a Microsoft Active Directory domain controller:*

1. Execute the following command to use the RFC2307 schema extension:

```
samba-tool domain provision --use-rfc2307 --interactive
```

2. Enable the schema update in a Samba domain controller. To do this, add the following line to the `/etc/samba/smb.conf` file:

```
dsdb:schema update allowed = true
```

If the schema update completes with an error, you need to perform a full restore of the domain controller that acts as a schema master.

If you want to poll a Samba domain controller correctly, you have to specify the `netbios` name and `workgroup` parameters in the `/etc/samba/smb.conf` file.

## Using VDI dynamic mode on client devices

A virtual infrastructure can be deployed on a corporate network using temporary virtual machines. Kaspersky Security Center Linux detects temporary virtual machines and adds information about them to the Administration Server database. After a user finishes using a temporary virtual machine, the machine is removed from the virtual infrastructure. However, a record about the removed virtual machine can be saved in the database of the Administration Server. Also, nonexistent virtual machines can be displayed in Kaspersky Security Center Web Console.

To prevent information about nonexistent virtual machines from being saved, Kaspersky Security Center Linux supports dynamic mode for Virtual Desktop Infrastructure (VDI). The administrator can enable support of [dynamic mode for VDI](#) in the properties of the installation package of Network Agent to be installed on the temporary virtual machine.

When a temporary virtual machine is disabled, Network Agent notifies the Administration Server that the machine has been disabled. If the virtual machine has been disabled successfully, it is removed from the list of devices connected to the Administration Server. If the virtual machine is disabled with errors and Network Agent does not send a notification about the disabled virtual machine to the Administration Server, a backup scenario is used. In this scenario, the virtual machine is removed from the list of devices connected to the Administration Server after three unsuccessful attempts to synchronize with the Administration Server.

## Enabling VDI dynamic mode in the properties of an installation package for Network Agent

*To enable VDI dynamic mode:*

1. In the main menu, go to **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.
2. In the context menu of the Network Agent installation package, select **Properties**.  
The **Properties** window opens.
3. In the **Properties** window, select the **Advanced** section.
4. In the **Advanced** section, select the **Enable dynamic mode for VDI** option.

The device on which Network Agent is to be installed becomes a part of VDI.

## Moving devices from VDI to an administration group

*To move devices that are part of VDI to an administration group:*

1. Go to **Assets (Devices)** → **Moving rules**.
2. Click **Add**.
3. On the **Rule conditions** tab, select the **Virtual machines** tab.
4. Set the **This is a virtual machine** rule to **Yes** and **Part of Virtual Desktop Infrastructure** to **Yes**.
5. Click **Save**.

# Deployment best practices

Kaspersky Security Center Linux is a distributed application. Kaspersky Security Center Linux includes the following applications:

- Administration Server—The core component, designed for managing devices of an organization and storing data in a DBMS.
- Kaspersky Security Center Web Console—The basic tool for the administrator. You can install Kaspersky Security Center Web Console either on the same device where Administration Server is installed or on another device.
- Network Agent—Designed for managing the security application installed on a device, as well as getting information about that device and transferring this information to the Administration Server. Network Agents are installed on devices of an organization.

Deployment of Kaspersky Security Center Linux on an organization's network is performed as follows:

- Installation of Administration Server
- Installation of Kaspersky Security Center Web Console on the administrator's device
- Installation of Network Agent and the security application on devices of the enterprise

## Hardening Guide

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

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

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

The Hardening Guide contains the following information:

- Selecting the Administration Server architecture
- Configuring a secure connection to Administration Server
- Configuring accounts to access Administration Server
- Managing protection of Administration Server
- Managing protection of client devices
- Configuring protection for managed applications
- Administration Server maintenance

- Transferring information to third-party applications

## Administration Server deployment

### Administration Server architecture

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

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

Based on this information, you can [form an architecture](#) that specifies:

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

### Selecting a device for the Administration Server installation

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

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

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

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

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

## Accounts for installing and running Administration Server

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

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

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

## Connection safety

### Usage of TLS

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

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

### Strict TLS settings

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

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

### Restricting access to the Administration Server database

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

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

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

By default, users can log in to Kaspersky Security Center Linux from any device where Kaspersky Security Center Web Console is installed. You can [configure Administration Server](#) so that users can connect to it only from devices with allowed IP addresses.



## Accounts and authentication

### Using two-step verification with Administration Server

Kaspersky Security Center Linux provides [two-step verification](#) for users of Kaspersky Security Center Web 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 Security Center Web Console, you enter your user name, password, and an additional single-use security code. To receive a single-use security code, you must install an authenticator application on your computer or your mobile device.

There are both software and hardware authenticators (tokens) that support the RFC 6238 standard. For example, software authenticators include Google Authenticator, Microsoft Authenticator, FreeOTP.

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

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

### Authentication of an internal user account

By default, the [password of an internal user account of Administration Server](#) must comply with the following rules:

- The password must be 8 to 16 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 attempts to enter a password is 10. You can [change the number of allowed password entry attempts](#).

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

## Dedicated administration group for Administration Server

We recommend [creating a dedicated administration group](#) for Administration Server. Grant this group [special access rights](#) and create a special security policy for it.

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

## Restricting the assignment of the Main Administrator role

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

## Configuring access rights to application features

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

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

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

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

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

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

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

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

## Separate account for remote installation of applications

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

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

## Regular audit of all users

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 possible compromise of the device.

# Managing protection of Administration Server

## Selecting an Administration Server protection software

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

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

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

- Kaspersky Industrial CyberSecurity for Nodes. We recommend installing this application on devices that are included in an industrial network. Kaspersky Industrial CyberSecurity for Nodes is an application that has certificates of compatibility with various manufacturers of industrial software.
- Recommended security products. If Administration Server is installed on a device with other software, we recommend taking into account the recommendations from that software vendor on the compatibility of security products (there may already be recommendations for selecting a security solution, and you may need to configure the trusted zone).

## Creating a separate security policy for the protection application

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

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

## Protection modules

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

## Configuring the firewall of the Administration Server device

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

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

## Managing protection of client devices

### Restricting of adding license keys to installation packages

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

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

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

### Automatic rules for moving devices between administration groups

We recommend restricting the use of [automatic rules for moving devices](#) between administration groups.

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

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

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

### Security requirements for distribution points and connection gateways

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

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

## Configuring protection for managed applications

### Managed application policies

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

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

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

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

The klmover utility allows you to manually connect a client device to the Administration Server. 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** also enables password protection for the Removal tool for Kaspersky Security Center Web Console (cleaner.exe).

## Using Kaspersky Security Network

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

## Regular scan of managed devices

For all device groups, we recommend [creating a task](#) that periodically runs a full scan of devices.

## Discovering new devices

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

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

## Administration Server maintenance

### Backup copying of Administration Server data

[Data backup](#) allows you to restore Administration Server data without data loss.

By default, a data backup task is created automatically after the installation of Administration Server and is executed periodically, saving backups in the appropriate directory. Settings of the data backup task can be changed as follows:

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

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

### Administration Server maintenance

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

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

- Checks the database for errors

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

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

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

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

## Event transfer to third-party systems

### Monitoring and reporting

For timely response to security issues, we recommend configuring the [monitoring and reporting features](#).

### Export of events to SIEM systems

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

### Email notifications of audit events

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

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

## Preparation for deployment

This section describes steps you must take before deploying Kaspersky Security Center Linux.

## Planning Kaspersky Security Center Linux deployment

This section provides information about the most convenient options for deployment of Kaspersky Security Center Linux components on an organization's network, depending on the following criteria:

- Total number of devices

- Units (local offices, branches) that are detached organizationally or geographically
- Separate networks connected by narrow channels
- Need for internet access to the Administration Server

## Typical schemes of protection system deployment

This section describes the standard deployment schemes of a protection system in an enterprise network using Kaspersky Security Center.

The system must be protected against any type of unauthorized access. We recommend that you install all available security updates for your operating system before installing the application on your device and physically protect Administration Server(s) and distribution point(s).

You can use Kaspersky Security Center to deploy a protection system on a corporate network by means of the following deployment schemes:

- Deploying a protection system through Kaspersky Security Center Web Console.  
Kaspersky applications are automatically installed on client devices, which in turn are automatically connected to the Administration Server by using Kaspersky Security Center.
- Deploying a protection system manually using stand-alone installation packages generated by Kaspersky Security Center.  
Installation of Kaspersky applications on client devices and the administrator's workstation is performed manually; the settings for connecting client devices to the Administration Server are specified when Network Agent is installed.  
This deployment method is recommended in cases when remote installation is not possible.

Kaspersky Security Center does not support deployment using Microsoft Active Directory® group policies.

## About planning Kaspersky Security Center Linux deployment in an organization's network

One Administration Server can support a maximum of 20,000 devices (with MariaDB as the DBMS). If the total number of devices on an organization's network exceeds 20,000, multiple Administration Servers must be deployed on that network and combined into a hierarchy for convenient centralized management.

If an organization includes large-scale remote local offices (branches) with their own administrators, it is useful to deploy Administration Servers in those offices. Otherwise, those offices must be viewed as detached networks connected by low-throughput channels; see section "[Standard configuration: A few large-scale offices run by their own administrators](#)".

When detached networks connected with narrow channels are used, traffic can be saved by assigning one or several Network Agents to act as distribution points (see [table for calculation of the number of distribution points](#)). In this case, all devices on a detached network retrieve updates from such local update centers. Actual distribution points can download updates both from the Administration Server (default scenario), and from Kaspersky servers on the internet (see section "[Standard configuration: Multiple small remote offices](#)").



Section "[Standard configurations of Kaspersky Security Center Linux](#)" provides detailed descriptions of the standard configurations of Kaspersky Security Center Linux. When planning the deployment, choose the most suitable standard configuration, depending on the organization's structure.

At the stage of deployment planning, the assignment of the special certificate X.509 to the Administration Server must be considered. Assignment of the X.509 certificate to the Administration Server may be useful in the following cases (partial list):

- Inspecting secure socket layer (SSL) traffic by means of an SSL termination proxy or for using a reverse proxy
- Specifying required values in certificate fields
- Providing the required encryption strength of a certificate

## Selecting a structure for protection of an enterprise

Selection of a structure for protection of an organization is defined by the following factors:

- Organization's network topology.
- Organizational structure.
- Number of employees in charge of the network protection, and allocation of their responsibilities.
- Hardware resources that can be allocated to protection management components.
- Throughput of communication channels that can be allocated to maintenance of protection components on the organizational network.
- Time limits for execution of critical administrative operations on the organization's network. Critical administrative operations include, for example, the distribution of anti-virus databases and modification of policies for client devices.

When you select a protection structure, it is recommended first to estimate the available network and hardware resources that can be used for the operation of a centralized protection system.

To analyze the network and hardware infrastructure, it is recommended that you follow the process below:

1. Define the following settings of the network on which the protection will be deployed:

- Number of network segments.
- Speed of communication channels between individual network segments.
- Number of managed devices in each of the network segments.
- Throughput of each communication channel that can be allocated to maintain the operation of the protection.

2. Determine the maximum allowed time for the execution of key administrative operations for all managed devices.

3. Analyze information from steps 1 and 2, as well as data from load testing of the administration system. Based on the analysis, answer the following questions:

- Is it possible to serve all the clients with a single Administration Server, or is a hierarchy of Administration Servers required?
- Which hardware configuration of Administration Servers is required in order to deal with all the clients within the time limits specified in step 2?
- Is it required to use distribution points to reduce load on communication channels?

Upon obtaining answers to the questions in step 3 above, you can compile a set of allowed structures of the organization's protection.

On the organization's network you can use one of the following standard protection structures:

- One Administration Server. All client devices are connected to a single Administration Server. Administration Server functions as distribution point.
- One Administration Server with distribution points. All client devices are connected to a single Administration Server. Some of the networked client devices function as distribution points.
- Hierarchy of Administration Servers. For each network segment, an individual Administration Server is allocated and becomes part of a general hierarchy of Administration Servers. The primary Administration Server functions as distribution point.
- Hierarchy of Administration Servers with distribution points. For each network segment, an individual Administration Server is allocated and becomes part of a general hierarchy of Administration Servers. Some of the networked client devices function as distribution points.

## Standard configurations of Kaspersky Security Center Linux

This section describes the following standard configurations used for deployment of Kaspersky Security Center Linux components on an organization's network:

- Single office
- A few large-scale offices, which are geographically detached and run by their own administrators
- Multiple small offices, which are geographically detached

### Standard configuration: Single office

One or several Administration Servers can be deployed on the organization's network. The number of Administration Servers can be selected either based on available hardware, or on the total number of managed devices.

One Administration Server can support up to 20,000 devices (with MariaDB as the DBMS). Consider the possibility of increasing the number of managed devices in the near future: it may be useful to connect a slightly smaller number of devices to a single Administration Server.

Administration Servers can be deployed either on the internal network, or in the DMZ, depending on whether internet access to the Administration Servers is required.

If multiple Servers are used, it is recommended that you combine them into a hierarchy. Using an Administration Server hierarchy allows you to avoid duplicated policies and tasks, and handle the whole set of managed devices as if they are managed by a single Administration Server (that is, search for devices, build selections of devices, and create reports).

## Standard configuration: A few large-scale offices run by their own administrators

If an organization has a few large-scale, geographically separate offices, you must consider the option of deploying Administration Servers at each of the offices. One or several Administration Servers can be deployed per office, depending on the number of client devices and hardware available. In this case, each of the offices can be viewed as a "[Standard configuration: Single office](#)". For ease of administration, it is recommended to combine all of the Administration Servers into a hierarchy (possibly multi-level).

If some employees move between offices with their devices (laptops), create Network Agent connection profiles in the Network Agent policy. Note that Network Agent connection profiles are only supported for Windows and macOS devices.

## Standard configuration: Multiple small remote offices

This standard configuration provides for a headquarters office and many remote small offices that may communicate with the HQ office over the internet. Each of the remote offices may be located behind a Network Address Translation (NAT), that is, no connection can be established between two remote offices because they are isolated.

An Administration Server must be deployed at the headquarters office, and one or multiple distribution points must be assigned to all other offices. If the offices are linked through the internet, it may be useful to create a *Download updates to the repositories of distribution points* task for the distribution points, so that they will download updates directly from Kaspersky servers, local or network folder, not from the Administration Server.

If some devices at a remote office have no direct access to the Administration Server (for example, access to the Administration Server is provided over the internet but some devices have no internet access), distribution points must be switched into connection gateway mode. In this case, Network Agents on devices at the remote office will be connected, for further synchronization, to the Administration Server—but through the gateway, not directly.

As the Administration Server, most probably, will not be able to poll the remote office network, it may be useful to turn this function over to a distribution point.

The Administration Server will not be able to send notifications to port 15000 UDP to managed devices located behind the NAT at the remote office. To resolve this issue, you can enable the mode of continuous connection to the Administration Server in the properties of devices acting as distribution points (**Do not disconnect from the Administration Server** check box). This mode is available if the total number of distribution points does not exceed 300. Use push servers to make sure that there is continuous connectivity between a managed device and the Administration Server. Refer to the following topic for details: [Enabling a push server](#).

## Selecting a DBMS

The following table lists the valid DBMS options, as well as the recommendations and restrictions on their use.

Recommendations and restrictions on DBMS

| DBMS | Recommendations and restrictions |
|------|----------------------------------|
|      |                                  |

|                                                                     |                                                                                                 |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| MySQL ( <a href="#">see supported versions</a> )                    | Use this DBMS if you intend to run a single Administration Server for less than 20,000 devices. |
| MariaDB ( <a href="#">see supported versions</a> )                  | Use this DBMS if you intend to run a single Administration Server for less than 20,000 devices. |
| PostgreSQL, Postgres Pro ( <a href="#">see supported versions</a> ) | Use this DBMS if you intend to run a single Administration Server for less than 50,000 devices. |

For information about how to install the selected DBMS, refer to its documentation.

It is recommended to disable the Software inventory task and disable (in the Kaspersky Endpoint Security policy settings) [notifications of Administration Server on started applications](#).

If you decide to install PostgreSQL or Postgres Pro DBMS, ensure that you specified a password for the superuser. If the password is not specified, Administration Server might not be able to connect to the database.

If you install [MariaDB](#), [PostgreSQL](#), or [Postgres Pro](#), use the recommended settings to ensure the DBMS functions properly.

## Providing internet access to Administration Server

The following cases require internet access to the Administration Server:

- Regular updating of Kaspersky databases, software modules, and applications
- Updating third-party software

By default, internet connection is not required for Administration Server to install Microsoft software updates on the managed devices. For example, the managed devices can download the Microsoft software updates directly from Microsoft Update servers or from Windows Server with Microsoft Windows Server Update Services (WSUS) deployed in your organization's network. Administration Server must be connected to the internet in the following cases:

- When you use Administration Server as WSUS server
- To install updates of third-party software other than Microsoft software
- Fixing third-party software vulnerabilities

Internet connection is required for Administration Server to perform the following tasks:

- To make a list of recommended fixes for vulnerabilities in Microsoft software. The list is created and regularly updated by Kaspersky specialists.
- To fix vulnerabilities in third-part software other than Microsoft software.
- Managing devices (laptops) of out-of-office users
- Managing devices in remote offices
- Interacting with primary or secondary Administration Servers located in remote offices
- Managing mobile devices

This section describes typical ways of providing access to the Administration Server over the internet. Each of the cases focusing on providing internet access to the Administration Server may require a dedicated certificate for the Administration Server.

## Internet access: Administration Server on a local network

If the Administration Server is located on the internal network of an organization, you might want to make TCP port 13000 of the Administration Server accessible from outside by means of port forwarding. If mobile device management is required, you might want to make accessible port 13292 TCP.

## Internet access: Administration Server in DMZ

If the Administration Server is located in the DMZ of the organization's network, it has no access to the organization's internal network. Therefore, the following limitations apply:

- The Administration Server cannot detect new devices.
- The Administration Server cannot perform initial deployment of Network Agent through forced installation on devices on the internal network of the organization.
- This only applies to the initial installation of Network Agent. Any further upgrades of Network Agent or the security application installation can, however, be performed by the Administration Server.

Note that Kaspersky Security Center Linux does not support deployment using group policies of Microsoft Windows.

You can use distribution points located on the organization's network. To perform initial deployment on devices without Network Agent, you first install Network Agent on one of the devices and then assign it the distribution point status. As a result, initial installation of Network Agent on other devices will be performed by the Administration Server through this distribution point.

To ensure a successful sending of notifications to port 15000 UDP on managed devices located on the internal network of the organization, you must cover the entire network with distribution points. In the properties of the distribution points that were assigned, select the **Do not disconnect from the Administration Server** check box. As a result, the Administration Server will establish a continuous connection to the distribution points while they will be able to send notifications to port 15000 UDP on devices that are on the [organization's internal network](#) (it can be an IPv4 or IPv6 network).

## Internet access: Network Agent as connection gateway in DMZ

Administration Server can be located on the internal network of the organization, and in that network's DMZ there can be a device with Network Agent running as a [connection gateway](#) with reverse connectivity (Administration Server establishes a connection to Network Agent). In this case, the following conditions must be met to ensure internet access:

- Network Agent must be [installed on the device](#) that is in the DMZ. When you install Network Agent, in the **Connection gateway** window of the setup wizard, select **Use Network Agent as a connection gateway in DMZ**.
- The device with the installed connection gateway must be added as a distribution point. When you add the connection gateway, in the **Add distribution point** window, select the **Select** → **Add connection gateway in**

**DMZ by address** option.

- To use an internet connection to connect external desktop computers to the Administration Server, the installation package for Network Agent must be corrected. In the properties of the created installation package, select the **Advanced** → **Connect to Administration Server by using a connection gateway** option, and then specify the newly created connection gateway.

For the connection gateway in the DMZ, Administration Server creates a certificate signed with the Administration Server certificate. If the administrator decides to assign a custom certificate to Administration Server, it must be done before a connection gateway is created in the DMZ.

If some employees use laptops that can connect to Administration Server either from the local network or over the internet, it may be useful to create a switching rule for Network Agent in the Network Agent's policy.

## About distribution points

A device with Network Agent installed can be used as a distribution point. In this mode, Network Agent can distribute updates, which can be retrieved either from the Administration Server or from Kaspersky servers. In the latter case, [configure update download for a distribution point](#).

Deployment of distribution points on an organization's network has the following objectives:

- Reducing the load on the Administration Server.
- Optimizing traffic.
- Providing the Administration Server with access to devices in hard-to-reach spots of the organization's network. The availability of a distribution point on the network behind a NAT (in relation to the Administration Server) allows the Administration Server to perform the following actions:
  - Send notifications to devices over UDP on the IPv4 or IPv6 network
  - Poll the IPv4 or IPv6 network
  - Perform initial deployment
  - Act as a [push server](#)

A distribution point is assigned for an administration group. In this case, the scope of the distribution point includes all devices within the administration group and all of its subgroups. However, the device that acts as the distribution point may not be included in the administration group to which it has been assigned.

You can make a distribution point function as a connection gateway. In this case, devices in the scope of the distribution point will be connected to the Administration Server through the gateway, not directly. This mode can be useful in scenarios that do not allow the establishment of a direct connection between the Administration Server and managed devices.

## Calculating the number and configuration of distribution points

The more client devices a network contains, the more distribution points it requires. We recommend that you not disable automatic assignment of distribution points. When automatic assignment of distribution points is enabled, Administration Server assigns distribution points if the number of client devices is quite large and defines their configuration.

## Using exclusively assigned distribution points

If you plan to use certain specific devices as distribution points (that is, exclusively assigned servers), you can opt out of using automatic assignment of distribution points. In this case, make sure that the devices that you intend to make distribution points have sufficient volume of [free disk space](#), are not shut down regularly, and have Sleep mode disabled.

Number of exclusively assigned distribution points on a network that contains a single network segment, based on the number of networked devices

| Number of client devices in the 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 exclusively assigned 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)                                                                   |
| 10–100                                       | 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 in the network segment | Number of distribution points                                                                            |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Less than 300                                   | 0 (Do not assign distribution points)                                                                    |
| More than 300                                   | $(N/300 + 1)$ , where N is the number of networked devices; there must be at least 3 distribution points |

Number of workstations functioning as distribution points on a network that contains multiple network segments, based on the number of networked devices

| Number of client devices per network segment | Number of distribution points                                                                            |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Less than 10                                 | 0 (Do not assign distribution points)                                                                    |
| 10–30                                        | 1                                                                                                        |
| 31–300                                       | 2                                                                                                        |
| More than 300                                | $(N/300 + 1)$ , where N is the number of networked devices; there must be at least 3 distribution points |

If a distribution point is shut down (or not available for some other reason), the managed devices in its scope can access the Administration Server for updates.

## Virtual Administration Servers

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

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

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

## Network settings for interaction with external services

Kaspersky Security Center Linux uses the following network settings for interacting with external services.

Network settings

| Network settings                       | Address                                                                                                                                                                                                                                                                                                                                                                 | Description                                                                       |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Port:<br>443<br><br>Protocol:<br>HTTPS | activation-<br>v2.kaspersky.com/activation-service/activation-service.svc                                                                                                                                                                                                                                                                                               | Application activation.                                                           |
| Port:<br>443<br><br>Protocol:<br>HTTPS | https://s00.upd.kaspersky.com<br>https://s01.upd.kaspersky.com<br>https://s02.upd.kaspersky.com<br>https://s03.upd.kaspersky.com<br>https://s04.upd.kaspersky.com<br>https://s05.upd.kaspersky.com<br>https://s06.upd.kaspersky.com<br>https://s07.upd.kaspersky.com<br>https://s08.upd.kaspersky.com<br>https://s09.upd.kaspersky.com<br>https://s10.upd.kaspersky.com | <a href="#">Updating Kaspersky databases, software modules, and applications.</a> |



|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                       | <p>https://s11.upd.kaspersky.com<br/> https://s12.upd.kaspersky.com<br/> https://s13.upd.kaspersky.com<br/> https://s14.upd.kaspersky.com<br/> https://s15.upd.kaspersky.com<br/> https://s16.upd.kaspersky.com<br/> https://s17.upd.kaspersky.com<br/> https://s18.upd.kaspersky.com<br/> https://s19.upd.kaspersky.com<br/> https://cm.k.kaspersky-labs.com</p>                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p>Port: 443<br/> Protocol: HTTPS</p> | <p>https://downloads.upd.kaspersky.com</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• <a href="#">Updating Kaspersky databases, software modules, and applications.</a></li> <li>• Checking if Kaspersky servers are accessible.<br/> Before downloading Kaspersky databases and software modules, Kaspersky Security Center Linux checks if Kaspersky servers are accessible. If access to the servers using system DNS is not possible, the application uses <a href="#">public DNS servers</a>.</li> </ul> |
| <p>Port: 80<br/> Protocol: HTTP</p>   | <p>http://p00.upd.kaspersky.com<br/> http://p01.upd.kaspersky.com<br/> http://p02.upd.kaspersky.com<br/> http://p03.upd.kaspersky.com<br/> http://p04.upd.kaspersky.com<br/> http://p05.upd.kaspersky.com<br/> http://p06.upd.kaspersky.com<br/> http://p07.upd.kaspersky.com<br/> http://p08.upd.kaspersky.com<br/> http://p09.upd.kaspersky.com<br/> http://p10.upd.kaspersky.com<br/> http://p11.upd.kaspersky.com<br/> http://p12.upd.kaspersky.com<br/> http://p13.upd.kaspersky.com<br/> http://p14.upd.kaspersky.com<br/> http://p15.upd.kaspersky.com<br/> http://p16.upd.kaspersky.com<br/> http://p17.upd.kaspersky.com<br/> http://p18.upd.kaspersky.com<br/> http://p19.upd.kaspersky.com<br/> http://downloads0.kaspersky-labs.com</p> | <p><a href="#">Updating Kaspersky databases, software modules, and applications.</a></p>                                                                                                                                                                                                                                                                                                                                                                         |

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                    |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
|                                    | <a href="http://downloads1.kaspersky-labs.com">http://downloads1.kaspersky-labs.com</a><br><a href="http://downloads2.kaspersky-labs.com">http://downloads2.kaspersky-labs.com</a><br><a href="http://downloads3.kaspersky-labs.com">http://downloads3.kaspersky-labs.com</a><br><a href="http://downloads4.kaspersky-labs.com">http://downloads4.kaspersky-labs.com</a><br><a href="http://downloads5.kaspersky-labs.com">http://downloads5.kaspersky-labs.com</a><br><a href="http://downloads6.kaspersky-labs.com">http://downloads6.kaspersky-labs.com</a><br><a href="http://downloads7.kaspersky-labs.com">http://downloads7.kaspersky-labs.com</a><br><a href="http://downloads8.kaspersky-labs.com">http://downloads8.kaspersky-labs.com</a><br><a href="http://downloads9.kaspersky-labs.com">http://downloads9.kaspersky-labs.com</a><br><a href="http://downloads.kaspersky-labs.com">http://downloads.kaspersky-labs.com</a><br><a href="http://cm.k.kaspersky-labs.com">http://cm.k.kaspersky-labs.com</a> |                                                    |
| Port: 443<br>Protocol: HTTPS       | ds.kaspersky.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Using <a href="#">Kaspersky Security Network</a> . |
| Port: 443, 1443<br>Protocol: HTTPS | <a href="http://ksn-a-stat-geo.kaspersky-labs.com">ksn-a-stat-geo.kaspersky-labs.com</a><br><a href="http://ksn-file-geo.kaspersky-labs.com">ksn-file-geo.kaspersky-labs.com</a><br><a href="http://ksn-verdict-geo.kaspersky-labs.com">ksn-verdict-geo.kaspersky-labs.com</a><br><a href="http://ksn-url-geo.kaspersky-labs.com">ksn-url-geo.kaspersky-labs.com</a><br><a href="http://ksn-a-p2p-geo.kaspersky-labs.com">ksn-a-p2p-geo.kaspersky-labs.com</a><br><a href="http://ksn-info-geo.kaspersky-labs.com">ksn-info-geo.kaspersky-labs.com</a><br><a href="http://ksn-cinfo-geo.kaspersky-labs.com">ksn-cinfo-geo.kaspersky-labs.com</a>                                                                                                                                                                                                                                                                                                                                                                        | Using <a href="#">Kaspersky Security Network</a> . |
| Protocol: HTTPS                    | <a href="http://click.kaspersky.com">click.kaspersky.com</a><br><a href="http://redirect.kaspersky.com">redirect.kaspersky.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Following links from the interface.                |
| Port: 80<br>Protocol: HTTP         | <a href="http://crl.kaspersky.com">http://crl.kaspersky.com</a><br><a href="http://ocsp.kaspersky.com">http://ocsp.kaspersky.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Public Key Infrastructure (PKI).                   |
| Port: 443<br>Protocol: HTTPS       | <a href="https://ipm-klca.kaspersky.com">https://ipm-klca.kaspersky.com</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <a href="#">Marketing announcements</a> .          |

For proper interaction of Kaspersky Security Center Linux with external services, consider the following recommendations:

- Unencrypted network traffic must be allowed on ports 443 and 1443 on the network equipment and proxy server of your organization.
- When Administration Server interacts with Kaspersky update servers and Kaspersky Security Network servers, it is necessary to avoid hijacking network traffic with certificate substitution ([MITM attacks](#)).

To download updates through the HTTP or HTTPS protocol by using the `klsclflag` utility:

1. Run the command line, and then change your current directory to the directory with the `klsclflag` utility. The `klsclflag` utility is located in the directory where the Administration Server is installed. The default installation path is `/opt/kaspersky/ksc64/sbin`.

2. If you want to download [updates](#) through the HTTP protocol, run one of the following commands under the root account:

- On the device with Administration Server installed:

```
klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
```

- On a distribution point:

```
klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
```

If you want to download [updates](#) through the HTTPS protocol, run one of the following commands under the root account:

- On the device with Administration Server installed:

```
klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
```

- On a distribution point:

```
klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
```

## Deploying Network Agent and the security application

To manage devices in an organization, you have to install Network Agent on each of them. Deployment of distributed Kaspersky Security Center Linux on corporate devices normally begins with installation of Network Agent on them.

In Microsoft Windows XP, Network Agent might not perform the following operations correctly: downloading updates directly from Kaspersky servers (as a distribution point) and functioning as a KSN proxy server (as a distribution point).

## Initial deployment

If a Network Agent has already been installed on a device, remote installation of applications on that device is performed through this Network Agent. The distribution package of an application to be installed is transferred over communication channels between Network Agents and Administration Server, along with the installation settings defined by the administrator. To transfer the distribution package, you can use relay distribution nodes, that is, distribution points, multicast delivery, etc. For more details on how to install applications on managed devices with Network Agent already installed, see below in this section.

You can perform initial installation of Network Agent on devices running Windows, using one of the following methods:

- With third-party tools for remote installation of applications.
- By cloning an image of the administrator's hard drive with the operating system and Network Agent: using tools provided by Kaspersky Security Center Linux for handling disk images, or using third-party tools.
- With Windows group policies: using standard Windows management tools for group policies, or in automatic mode, through the corresponding, dedicated option in the remote installation task of Kaspersky Security Center Linux.

- In forced mode, using special options in the remote installation task of Kaspersky Security Center Linux.
- By sending device users links to stand-alone packages generated by Kaspersky Security Center Linux. Stand-alone packages are executable modules that contain the distribution packages of selected applications with their settings defined.
- Manually, by running application installers on devices.

On platforms other than Microsoft Windows, initial installation of Network Agent on managed devices must be performed through available third-party tools. You can upgrade Network Agent to a new version or install other Kaspersky applications on non-Windows platforms, using Network Agents (already installed on devices) to perform remote installation tasks. In this case, installation is identical to that on devices running Microsoft Windows.

When selecting a method and a strategy for deployment of applications on a managed network, you must consider a number of factors (partial list):

- [Organization's network](#) configuration.
- Total number of devices.
- Presence of devices on the organization's network, which are not members of any Active Directory domain, and presence of uniform accounts with administrator rights on those devices.
- Capacity of the channel between the Administration Server and devices.
- Type of communication between Administration Server and remote subnets and capacity of network channels in those subnets.
- Security settings applied on remote devices at the start of deployment (such as use of UAC and Simple File Sharing mode).

## Configuring installers

Before starting deployment of Kaspersky applications on a network, you must specify the installation settings, that is, those defined during the application installation. When installing Network Agent, you should specify, at a minimum, an address for connection to Administration Server; some advanced settings may also be required. Depending on the installation method that you have selected, you can define settings in different ways. In the simplest case (manual interactive installation on a selected device), all relevant settings can be defined through the user interface of the installer.

This method of defining the settings is inappropriate for silent installation of applications on groups of devices. In general, the administrator must specify values for settings in centralized mode; those values can subsequently be used for silent installation on selected networked devices.

## Installation packages

The first and main method of defining the installation settings of applications is all-purpose and thus suitable for all installation methods, both with Kaspersky Security Center Linux tools, and with most third-party tools. This method consists of creating installation packages of applications in Kaspersky Security Center Linux.

Installation packages are generated using the following methods:

- Automatically, from specified distribution packages, on the basis of included *descriptors* (files with the *kud* extension that contain rules for installation and results analysis, and other information)
- From the executable files of installers or from installers in native format (.msi, .deb, .rpm), for standard or supported applications

Generated installation packages are organized hierarchically as folders with subfolders and files. In addition to the original distribution package, an installation package contains editable settings (including the installer's settings and rules for processing such cases as necessity of restarting the operating system in order to complete installation), as well as minor auxiliary modules.

Values of installation settings that would be specific for an individual supported application can be defined in the user interface of Kaspersky Security Center Web Console when the installation package is created. When performing remote installation of applications through Kaspersky Security Center Linux tools, installation packages are delivered to devices so that running the installer of an application makes all administrator-defined settings available for that application. When using third-party tools for installation of Kaspersky applications, you only have to ensure the availability of the entire installation package on the device, that is, the availability of the distribution package and its settings. Installation packages are created and stored by Kaspersky Security Center Linux in a dedicated subfolder [of the shared folder](#).

Do not specify any details of privileged accounts in the parameters of installation packages.

Deployment using group policies of Microsoft Windows is not supported.

Immediately after Kaspersky Security Center Linux installation, a few installation packages are automatically generated; they are ready for installation and include Network Agent packages and security application packages for Microsoft Windows.

Although the license key for an application can be set in the properties of an installation package, it is advisable to avoid this method of license distribution because there it is easy to obtain read access to installation packages. You should use automatically distributed license keys or installation tasks for license keys.

## About remote installation tasks in Kaspersky Security Center Linux

Kaspersky Security Center Linux provides various mechanisms for remote installation of applications, which are implemented as remote installation tasks (forced installation, installation by copying a hard drive image). You can create a remote installation task both for a specified administration group and for specific devices or a selection of devices (such tasks are displayed in Kaspersky Security Center Web Console, in the **Tasks** folder). When creating a task, you can select installation packages (those of Network Agent and / or another application) to be installed within this task, as well as specify certain settings that define the method of remote installation. In addition, you can use the Remote installation wizard, which is based on creation of a remote installation task and results monitoring.

Tasks for administration groups affect both devices included in a specified group and all devices in all subgroups within that administration group. A task covers devices of secondary Administration Servers included in a group or any of its subgroups if the corresponding setting is enabled in the task.

Tasks for specific devices refresh the list of client devices at each run in accordance with the selection contents at the moment the task starts. If a selection includes devices that have been connected to secondary Administration Servers, the task will run on those devices, too. For details on those settings and installation methods see below in this section.

To ensure a successful operation of a remote installation task on devices connected to secondary Administration Servers, you must use the relaying task to relay installation packages used by your task to corresponding secondary Administration Servers in advance.

## Deployment by capturing and copying the image of a device

If you need to install Network Agent on devices on which an operating system and other software also must be installed (or reinstalled), you can use the mechanism of capturing and copying the image of that device.

*To perform deployment by capturing and copying a hard drive:*

1. Create a reference device with an operating system and the relevant software installed, including Network Agent and a security application.
2. Capture the reference image on the device and distribute that image on new devices through the dedicated task of Kaspersky Security Center Linux.

To capture and install disk images, use third-party tools available in the organization.

### Copying a disk image with third-party tools

When applying third-party tools for capturing the image of a device with Network Agent installed, use one of the following methods:

- On the reference device, stop the Network Agent service and run the `klmover` utility with the `-dupfix` key. The utility `klmover` is included in the installation package of Network Agent. Avoid any subsequent runs of Network Agent service until the image capturing operation completes.
- Make sure that `klmover` 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.
- [Use the Network Agent disk cloning mode.](#)

If the hard drive image has been copied incorrectly, you can resolve this problem.

You can also capture the image of a device without Network Agent installed. To do this, perform image deployment on target devices and then deploy Network Agent. If using this method, provide access to the network folder with stand-alone installation packages from a device.

## Network Agent disk cloning mode

Cloning the hard drive of a reference device is a popular method of software installation on new devices. If Network Agent is running in standard mode on the hard drive of the reference device, the following problem arises:

After the reference disk image with Network Agent is deployed on new devices, they are displayed in Kaspersky Security Center Web Console as a single device. This problem arises because the cloning procedure causes new devices to keep identical internal data, which allows the Administration Server to associate a device with its own record in Kaspersky Security Center Web Console.

The special *Network Agent disk cloning mode* allows you to avoid problems with an incorrect display of new devices in Kaspersky Security Center Web Console after cloning. Use this mode when you deploy software (with Network Agent) on new devices by cloning the disk.

In disk cloning mode, Network Agent keeps running but does not connect to the Administration Server. When exiting the cloning mode, Network Agent deletes the internal data, which causes Administration Server to associate multiple devices with a single record in Kaspersky Security Center Web Console. Upon completing the cloning of the reference device image, new devices are displayed in Kaspersky Security Center Web Console properly (under individual records).

## Network Agent disk cloning mode use scenario

1. The administrator installs Network Agent on the reference device.
2. The administrator checks the Network Agent connection to the Administration Server using the `klmagchk` utility.
3. The administrator enables the Network Agent disk cloning mode.
4. The administrator installs software and patches on the device, and restarts it as many times as needed.
5. The administrator clones the hard drive of the reference device on any number of devices.
6. Each cloned copy must meet the following conditions:
  - a. The device name must be changed.
  - b. The device must be restarted.
  - c. The disk cloning mode must be disabled.

## Enabling and disabling the disk cloning mode using the `klmover` utility

*To enable or disable the Network Agent disk cloning mode:*

1. Run the `klmover` utility on the device with Network Agent installed that you have to clone.  
The `klmover` utility is located in the Network Agent installation folder.
2. To enable the disk cloning mode, enter the following command at the Windows command prompt: `klmover -cloningmode 1`.  
Network Agent switches to disk cloning mode.
3. To request the current status of the disk cloning mode, enter the following command at the command prompt: `klmover -cloningmode`.  
The utility window shows whether the disk cloning mode is enabled or disabled.

4. To disable the disk cloning mode, enter the following command in the utility command line: `k1mover -cloningmode 0`.

## Forced deployment through the remote installation task of Kaspersky Security Center Linux

If you need to start deploying Network Agents or other applications immediately, without waiting for the next time target devices log in to the domain, or if any target devices that are not members of the Active Directory domain are available, you can force installation of selected installation packages through the remote installation task of Kaspersky Security Center Linux.

In this case, you can specify target devices either explicitly (with a list), or by selecting the Kaspersky Security Center Linux administration group to which they belong, or by creating a selection of devices based upon a specific criterion. The installation start time is defined by the task schedule. If the **Run missed tasks** setting is enabled in the task properties, the task can be run either immediately after target devices are turned on, or when they are moved to the target administration group.

This type of installation consists in copying files to the administrative resource (admin\$) on each device and performing remote registration of supporting services on them. Only designated distribution points can perform forced deployment on Windows devices from the administrative resource. The following conditions must be met in this case:

- Devices must be available for connection either from the Administration Server side, or from the distribution point side.
- Name resolution for target devices must function properly in the network.
- The administrative shares (admin\$) must remain enabled on target devices.
- The Server system service must be running on target devices (by default, it is running).
- The following ports must be open on target devices to allow remote access through Windows tools: TCP 139, TCP 445, UDP 137, and UDP 138.
- Simple File Sharing mode must be disabled on target devices.
- On target devices, the access sharing and security model must be set as *Classic – local users authenticate as themselves*, it can be in no way *Guest only – local users authenticate as Guest*.
- Target devices must be members of the domain, or uniform accounts with administrator rights must be created on target devices in advance.

Devices in workgroups can be adjusted in accordance with the above requirements by using the riprep utility, which is described [on Kaspersky Technical Support website](#).

During installation on new devices that have not yet been allocated to any of the Kaspersky Security Center Linux administration groups, you can open the remote installation task properties and specify the administration group to which devices will be moved after Network Agent installation.

When creating a group task, keep in mind that each group task affects all devices in all nested groups within a selected group. Therefore, you must avoid duplicating installation tasks in subgroups.



Automatic installation is a simplified way to create tasks for forced installation of applications. To do this, open the administration group properties, open the list of installation packages and 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.

Forced installation can also be applied if devices cannot be directly accessed by the Administration Server: for example, devices are on isolated networks, or they are on a local network while the Administration Server item is in DMZ. To make forced installation possible, you must provide distribution points to each of the isolated networks.

Using distribution points as local installation centers may also be useful when performing installation on devices in subnets communicated with Administration Server via a low-capacity channel while a broader channel is available between devices in the same subnet. However, note that this installation method places a significant load on devices acting as distribution points. Therefore, it is recommended that you select powerful devices with high-performance storage units as distribution points. Moreover, the free disk space in the partition with the `/var/opt/kaspersky/klnagent_srv/` folder must exceed, by many times, the total size of the [distribution packages of installed applications](#).

## Running stand-alone packages created by Kaspersky Security Center Linux

The above-described methods of initial deployment of Network Agent and other applications cannot always be implemented because it is not possible to meet all of the applicable conditions. In such cases, you can create a common executable file called a *stand-alone installation package* through Kaspersky Security Center Linux, using installation packages with the relevant installation settings that have been prepared by the administrator. The stand-alone installation package is stored in the shared folder of Kaspersky Security Center Linux.

You can use Kaspersky Security Center Linux to send selected users an email message containing a link to this file in the shared folder, prompting them to run the file (either in interactive mode, or with the key "-s" for silent installation). You can attach the stand-alone installation package to an email message and then send it to the users of devices that have no access to the shared folder of Kaspersky Security Center Linux. The administrator can also copy the stand-alone package to a removable drive, deliver it to a relevant device, and then run it later.

You can create a stand-alone package from a Network Agent package, a package of another application (for example, the security application), or both. If the stand-alone package has been created from Network Agent and another application, installation starts with Network Agent.

When creating a stand-alone package with Network Agent, you can specify the administration group to which new devices (those that have not been allocated to any of the administration groups) will be automatically moved when Network Agent installation completes on them.

Stand-alone packages can run in interactive mode (by default), displaying the result for installation of applications they contain, or they can run in silent mode (when run with the key "-s"). Silent mode can be used for installation from scripts, for example, from scripts configured to run after an operating system image is deployed. The result of installation in silent mode is determined by the return code of the process.

## Remote installation of applications on devices with Network Agent installed

If an operable Network Agent connected to the primary Administration Server (or to any of its secondary Servers) is installed on a device, you can upgrade Network Agent on this device, as well as install, upgrade, or remove any supported applications through Network Agent.

You can enable the **Using Network Agent** option in the properties of the [remote installation task](#).

If this option is selected, installation packages with installation settings defined by the administrator will be transferred to target devices over communication channels between Network Agent and the Administration Server.

To optimize the load on the Administration Server and minimize traffic between the Administration Server and the devices, it is useful to assign distribution points on every remote network or in every broadcasting domain (see sections "[About distribution points](#)" and "[Building a structure of administration groups and assigning distribution points](#)"). In this case, installation packages and the installer settings are distributed from the Administration Server to target devices through distribution points.

Moreover, you can use distribution points for broadcasting (multicast) delivery of installation packages, which allows reducing network traffic significantly when deploying applications.

When transferring installation packages to target devices over communication channels between Network Agents and the Administration Server, all installation packages that have been prepared for transfer will also be cached in the `/var/opt/kaspersky/klagent_srv/1093/.working/` folder. When using multiple large installation packages of various types and involving a large number of distribution points, the size of this folder may increase dramatically.

Files cannot be deleted from the FTServer folder manually. When original installation packages are deleted, the corresponding data will be automatically deleted from the FTServer folder.

The data received by distribution points is saved in the folder `/var/opt/kaspersky/klagent_srv/1103/`.

Files cannot be deleted from the \$FTCITmp folder manually. As tasks using data from this folder complete, the contents of this folder will be deleted automatically.

Because installation packages are distributed over communication channels between Administration Server and Network Agents from an intermediate repository in a format optimized for network transfers, no changes are allowed in installation packages stored in the original folder of each installation package. Those changes will not be automatically registered by Administration Server. If you need to modify the files of installation packages manually (although you are recommended to avoid this scenario), you must edit any of the settings of an installation package in Kaspersky Security Center Web Console. Editing the settings of an installation package in Kaspersky Security Center Web Console causes Administration Server to update the package image in the cache that has been prepared for transfer to target devices.

## Managing device restarts in the remote installation task

Devices often need a restart to complete the remote installation of applications (particularly on Windows).

If you use the remote installation task of Kaspersky Security Center Linux, in the New task wizard or in the properties window of the task that has been created (**Operating system restart** section), you can select the action to perform when the Windows device requires a restart:

- **Do not restart the device.** In this case, no automatic restart will be performed. To complete the installation, you must restart the device (for example, manually or through the device management task). Information about the required restart will be saved in the task results and in the device status. This option is suitable for installation tasks on servers and other devices where continuous operation is critical.
- **Restart the device.** In this case, the device is always restarted automatically if a restart is required for completion of the installation. This option is useful for installation tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- **Prompt user for action.** In this case, the restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). The **Prompt user for action** is the most suitable for workstations where users need a possibility of selecting the most convenient time for a restart.

## Suitability of databases updating in an installation package of a security application

Before starting the protection deployment, you must keep in mind the possibility of updating anti-virus databases (including modules of automatic patches) shipped together with the distribution package of the security application. It is useful to update the databases in the installation package of the application before starting the deployment (for example, by using the corresponding command in the context menu of a selected installation package). This will reduce the number of restarts required for completion of protection deployment on target devices.

## Monitoring the deployment

To monitor the Kaspersky Security Center Linux deployment and make sure that a security application and Network Agent are installed on managed devices, [use the monitoring and reporting feature](#):

- Use the deployment widget of the [dashboard](#) to monitor deployment in real time.
- Use [reports](#) to get detailed information.

## Configuring installers

This section provides information about the files of Kaspersky Security Center Linux installers and the installation settings, as well as recommendations on how to install Administration Server and Network Agent in silent mode.

## General information

Installers of Kaspersky Security Center Linux components for Windows devices are built on Windows Installer technology. An MSI package is the core of an installer. This format of packaging allows using all of the advantages provided by Windows Installer: scalability, availability of a patching system, transformation system, centralized installation through third-party solutions, and transparent registration with the operating system.

## Installation in silent mode (with a response file)

The installer of Network Agent has the feature of working with the response file (ss\_install.xml), where the parameters for installation in silent mode without user participation are integrated. The ss\_install.xml file is located in the same folder as the MSI package; it is used automatically during installation in silent mode. You can enable the silent installation mode with the command line key "/s".

An overview of an example run follows:

```
setup.exe /s
```

Before you start the installer in silent mode, read the End User License Agreement (EULA). If the Kaspersky Security Center Linux distribution kit does not include a TXT file with the text of the EULA, you can download the file from the [Kaspersky website](#).

The ss\_install.xml file is an instance of the internal format of parameters of the Kaspersky Security Center Linux installer. Distribution packages contain the ss\_install.xml file with the default parameters.

Please do not modify the ss\_install.xml file manually. This file can be modified through the tools of Kaspersky Security Center Linux, when editing the parameters of the installation packages in Kaspersky Security Center Web Console.

## Partial installation configuration through setup.exe

When running installation of applications through setup.exe, you can add the values of any properties of MSI to the MSI package.

This command appears as follows:

Example:

```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

## Administration Server installation parameters

The table below describes the properties that you can configure when installing Kaspersky Security Center Linux in silent mode.

Parameters of Administration Server installation in silent mode

| Variable name             | Required | Description                                                                          | Possible values        |
|---------------------------|----------|--------------------------------------------------------------------------------------|------------------------|
| EULA_ACCEPTED             | Yes      | Confirms that you understand and accept the terms of the End User License Agreement. | 1                      |
| PP_ACCEPTED               | Yes      | Confirms that you understand and accept the terms of the Privacy Policy.             | 1                      |
| KLSRV_UNATT_SERVERADDRESS | Yes      | The Administration Server DNS-name or static IP address.                             | DNS name or IP address |
| KLSRV_UNATT_PORT_SRV      | No       | The Administration Server port number. Optional, default value is 14000.             | Port number            |

|                           |     |                                                                                                                                                                  |                                                                                                           |
|---------------------------|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| KLSRV_UNATT_PORT_SRV_SSL  | No  | The Administration Server SSL port number. Optional, default value is 13000.                                                                                     | Port number                                                                                               |
| KLSRV_UNATT_PORT_KLOAPI   | No  | The Administration Server KLOAPI port number. Optional, default value is 13299.                                                                                  | Port number                                                                                               |
| KLSRV_UNATT_PORT_GUI      | No  | The Administration Server GUI port number. Optional, default value is 13291.                                                                                     | Port number                                                                                               |
| KLSRV_UNATT_NETRANGETYPE  | No  | The approximate number of devices that you intend to manage. Optional, default value is 1.                                                                       | 1 for 1 to 100 netw devices.<br>2 for 101 to 1000 networked device<br>3 for more than 10 networked device |
| KLSRV_UNATT_DBMS_TYPE     | Yes | The database management system type: MySQL (MariaDB) or Postgres.                                                                                                | mysql<br>or<br>postgres                                                                                   |
| KLSRV_UNATT_DBMS_INSTANCE | Yes | The database server IP address.                                                                                                                                  | IP address                                                                                                |
| KLSRV_UNATT_DBMS_PORT     | Yes | The database server port. Default value for MySQL (MariaDB) is 3306; default value for Postgres is 5432.                                                         | 3306<br>or<br>5432                                                                                        |
| KLSRV_UNATT_DB_NAME       | Yes | The database name.                                                                                                                                               | kav                                                                                                       |
| KLSRV_UNATT_DBMS_LOGIN    | Yes | The username of a user that has access to the database.                                                                                                          |                                                                                                           |
| KLSRV_UNATT_DBMS_PASSWORD | Yes | The password of a user that has access to the database.                                                                                                          |                                                                                                           |
| KLSRV_UNATT_KLADMINSGROUP | Yes | The security group name for services.                                                                                                                            | kladmins                                                                                                  |
| KLSRV_UNATT_KLSRVUSER     | Yes | The account name to start the Administration Server service. The account must be a member of the security group specified in KLSRV_UNATT_KLADMINSGROUP variable. | ksc                                                                                                       |
| KLSRV_UNATT_KLSVCUSER     | Yes | The account name to start other services. The account must be a member of the security group specified in KLSRV_UNATT_KLADMINSGROUP variable.                    | ksc                                                                                                       |

If the Administration Server is to be deployed as a [Kaspersky Security Center Linux failover cluster](#), the answer file include the following additional variables:

|                                    |     |                              |              |
|------------------------------------|-----|------------------------------|--------------|
| KLFOC_UNATT_NODE                   | Yes | The node number (1 or 2).    | 1<br>or<br>2 |
| KLFOC_UNATT_STATE_SHARE_MOUNT_PATH | Yes | The state share mount point. |              |

|                                                                                                                                       |                                    |                                           |                                        |
|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-------------------------------------------|----------------------------------------|
| KLFOC_UNATT_DATA_SHARE_MOUNT_PATH                                                                                                     | Yes                                | The data share mount point.               |                                        |
| KLFOC_UNATT_CONN_MODE                                                                                                                 | Yes                                | The failover cluster connectivity mode.   | VirtualAdapter<br>or<br>ExternalLoadBa |
| In case the KLFOC_UNATT_CONN_MODE variable has VirtualAdapter value, the answer file must include the following additional variables: |                                    |                                           |                                        |
| KLFOC_UNATT_CONN_MODE_VA_NAME                                                                                                         |                                    | The virtual network adapter name.         |                                        |
| KLFOC_UNATT_CONN_MODE_VA_IPV4                                                                                                         | One of these variables is required | The virtual network adapter IP address.   | IP address                             |
| KLFOC_UNATT_CONN_MODE_VA_IPV6                                                                                                         |                                    | The virtual network adapter IPv6 address. | IPv6 address                           |

## Network Agent installation parameters

The table below describes the MSI properties that you can configure when installing Network Agent. All of the parameters are optional, except for EULA and SERVERADDRESS.

Parameters of Network Agent installation in silent mode

| MSI property         | Description                                      | Available values                                                                                                                                                                                                                                                                                                                                               |
|----------------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EULA                 | Acceptance of the terms of the License Agreement | <ul style="list-style-type: none"> <li>1—I have fully read, understand and accept the terms of the <a href="#">End User License Agreement</a>.</li> <li>0—I do not accept the terms of the License Agreement (installation is not performed).</li> <li>No value—I do not accept the terms of the License Agreement (installation is not performed).</li> </ul> |
| DONT_USE_ANSWER_FILE | Read installation settings from response file    | <ul style="list-style-type: none"> <li>1—Do not use.</li> <li>Other value or no value—Read.</li> </ul>                                                                                                                                                                                                                                                         |
| INSTALLDIR           | Path to the Network Agent installation folder    | String value.                                                                                                                                                                                                                                                                                                                                                  |
|                      |                                                  |                                                                                                                                                                                                                                                                                                                                                                |

|                                           |                                                                                                                                                                              |                                                                                                                                                                                                                             |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SERVERADDRESS                             | Administration Server address (required)                                                                                                                                     | String value.                                                                                                                                                                                                               |
| SERVERPORT                                | Number of port for connection to Administration Server                                                                                                                       | Numerical value.                                                                                                                                                                                                            |
| SERVERSSLPORT                             | Number of the port for encrypted connection to Administration Server by using SSL protocol                                                                                   | Numerical value.                                                                                                                                                                                                            |
| USESSL                                    | Whether to use SSL connection                                                                                                                                                | <ul style="list-style-type: none"> <li>• 1—Use.</li> <li>• Other value or no value—Do not use.</li> </ul>                                                                                                                   |
| OPENUDPPOINT                              | Whether to open a UDP port                                                                                                                                                   | <ul style="list-style-type: none"> <li>• 1—Open.</li> <li>• Other value or no value—Do not open.</li> </ul>                                                                                                                 |
| UDPPOINT                                  | UDP port number                                                                                                                                                              | Numerical value.                                                                                                                                                                                                            |
| USEPROXY                                  | Whether to use a proxy server.<br>For compatibility purposes, it is not recommended to specify proxy connection settings in the Network Agent installation package settings. | <ul style="list-style-type: none"> <li>• 1—Use.</li> <li>• Other value or no value—Do not use.</li> </ul>                                                                                                                   |
| PROXYLOCATION<br>(PROXYADDRESS:PROXYPORT) | Proxy address and number of port for connection to proxy server                                                                                                              | String value.                                                                                                                                                                                                               |
| PROXYLOGIN                                | Account for connection to proxy server                                                                                                                                       | String value.                                                                                                                                                                                                               |
| PROXYPASSWORD                             | Password of account for connection to proxy server (Do not specify any details of privileged accounts in the parameters of installation packages.)                           | String value.                                                                                                                                                                                                               |
| GATEWAYMODE                               | Connection gateway use mode                                                                                                                                                  | <ul style="list-style-type: none"> <li>• 0—Do not use connection gateway.</li> <li>• 1—Use this Network Agent as connection gateway.</li> <li>• 2—Connect to the Administration Server using connection gateway.</li> </ul> |
| GATEWAYADDRESS                            | Connection gateway address                                                                                                                                                   | String value.                                                                                                                                                                                                               |
| CERTSELECTION                             | Method of receiving a certificate                                                                                                                                            | <ul style="list-style-type: none"> <li>• GetOnFirstConnection—Receive a certificate from the Administration Server.</li> <li>• GetExistent—Select an existing certificate. If this option is selected, the</li> </ul>       |

|               |                                                                              |                                                                                                                              |
|---------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                              | CERTFILE property must be specified.                                                                                         |
| CERTFILE      | Path to the certificate file                                                 | String value.                                                                                                                |
| VMVDI         | Enable dynamic mode for Virtual Desktop Infrastructure (VDI)                 | <ul style="list-style-type: none"> <li>• 1—Enable.</li> <li>• 0—Do not enable.</li> <li>• No value—Do not enable.</li> </ul> |
| LAUNCHPROGRAM | Whether to start the Network Agent service after installation                | <ul style="list-style-type: none"> <li>• 1—Start.</li> <li>• Other value or no value—Do not start.</li> </ul>                |
| NAGENTTAGS    | Tag for Network Agent (has priority over the tag given in the response file) | String value.                                                                                                                |

## Virtual infrastructure

Kaspersky Security Center Linux supports the use of virtual machines. You can install Network Agent and the security application on each virtual machine, and you can protect virtual machines at the hypervisor level. In the first case, you can use either a standard security application or [Kaspersky Security for Virtualization Light Agent](#) to protect your virtual machines. In the second case, you can use [Kaspersky Security for Virtualization Agentless](#).

Kaspersky Security Center Linux supports rollbacks of virtual machines to their [previous state](#).

## Tips on reducing the load on virtual machines

When installing Network Agent on a virtual machine, you are advised to consider disabling some Kaspersky Security Center Linux features that seem to be of little use for virtual machines.

When installing Network Agent on a virtual machine or on a template intended for generation of virtual machines, we recommend the following actions:

- If you are running a remote installation, in the properties window of the Network Agent installation package, in the **Advanced** section, select the **Optimize settings for VDI** option.
- If you are running an interactive installation through a wizard, in the wizard window, select the **Optimize the Network Agent settings for the virtual infrastructure** option.

Selecting those options alters the settings of Network Agent so that the following features remain disabled by default (before a policy is applied):

- Retrieving information about software installed
- Retrieving information about hardware



- Retrieving information about vulnerabilities detected
- Retrieving information about updates required

Usually, those features are not necessary on virtual machines because they use uniform software and virtual hardware.

Disabling the features is invertible. If any of the disabled features is required, you can enable it through the policy of Network Agent, or through the local settings of Network Agent. The local settings of Network Agent are available through the context menu of the relevant device in Kaspersky Security Center Web Console.

## Support of dynamic virtual machines

Kaspersky Security Center Linux supports dynamic virtual machines. If a virtual infrastructure has been deployed on the organization's network, dynamic (temporary) virtual machines can be used in certain cases. The dynamic VMs are created under unique names based on a template that has been prepared by the administrator. The user works on a VM for a while and then, after being turned off, this virtual machine will be removed from the virtual infrastructure. If Kaspersky Security Center Linux has been deployed on the organization's network, a virtual machine with installed Network Agent will be added to the Administration Server database. After you turn off a virtual machine, the corresponding entry must also be removed from the database of Administration Server.

To make functional the feature of automatic removal of entries on virtual machines, when installing Network Agent on a template for dynamic virtual machines, select the **Enable dynamic mode for VDI** option:

- For remote installation—In the [properties window of the installation package of Network Agent \(Advanced section\)](#).
- For interactive installation—In the Network Agent installation wizard

Avoid selecting the **Enable dynamic mode for VDI** option when installing Network Agent on physical devices.

If you want events from dynamic virtual machines to be stored on the Administration Server for a while after you remove those virtual machines, then, in the Administration Server properties window, in the **Events repository** section, select the **Store events after devices are deleted** option and specify the maximum storage term for events (in days).

## Support of virtual machines copying

Copying a virtual machine with installed Network Agent or creating one from a template with installed Network Agent is identical to the deployment of Network Agents by capturing and copying a hard drive image. So, in general case, when copying virtual machines, you need to perform the same actions as when [deploying Network Agent by copying a disk image](#).

However, the two cases described below showcase Network Agent, which detects the copying automatically. Owing to the above reasons, you do not have to perform the sophisticated operations described under "Deployment by capturing and copying the hard drive of a device":

- The **Enable dynamic mode for VDI** option was selected when Network Agent was installed—After each restart of the operating system, this virtual machine will be recognized as a new device, regardless of whether it has been copied or not.

- One of the following hypervisors is in use: VMware™, HyperV®, or Xen®: Network Agent detects the copying of the virtual machine by the changed IDs of the virtual hardware.

Analysis of changes in virtual hardware is not absolutely reliable. Before applying this method widely, you must test it on a small pool of virtual machines for the version of the hypervisor currently used in your organization.

## Support of file system rollback for devices with Network Agent

Kaspersky Security Center Linux is a distributed application. Rolling back the file system to a previous state on a device with Network Agent installed will lead to data desynchronization and improper functioning of Kaspersky Security Center Linux.

The file system (or a part of it) can be rolled back in the following cases:

- When copying an image of the hard drive.
- When restoring a state of the virtual machine by means of the virtual infrastructure.
- When restoring data from a backup copy or a recovery point.

Scenarios under which third-party software on devices with Network Agent installed affects the %ALLUSERSPROFILE%\Application Data\KasperskyLab\admindit\ folder are only critical scenarios for Kaspersky Security Center Linux. Therefore, you must always exclude this folder from the recovery procedure, if possible.

Because the workplace rules of some organizations provide for rollbacks of the file system on devices, support for the file system rollback on devices with Network Agent installed has been added to Kaspersky Security Center Linux, starting with version 10 Maintenance Release 1 (Administration Server and Network Agents must be of version 10 Maintenance Release 1 or later). When detected, those devices are automatically reconnected to the Administration Server with full data cleansing and full synchronization.

By default, support of file system rollback detection is enabled in Kaspersky Security Center Linux.

As much as possible, avoid rolling back the %ALLUSERSPROFILE%\Application Data\KasperskyLab\admindit\ folder on devices with Network Agent installed, because full resynchronization of data requires a large amount of resources.

A rollback of the system state is absolutely not allowed on a device with Administration Server installed. Nor is a rollback of the database used by Administration Server.

You can restore a state of Administration Server from a backup copy only with the standard kbackup utility.

## Local installation of applications

This section provides an installation procedure for applications that can be installed on local devices only.

To perform local installation of applications on a specific client device, you must have administrator rights on this device.

*To install applications locally on a specific client device:*

1. Install Network Agent on the client device and configure the connection between the client device and Administration Server.
2. Install the requisite applications on the device as described in the guides of these applications.
3. Install a management plug-in for each of the installed applications on the administrator's workstation.

Kaspersky Security Center Linux also supports the option of local installation of applications using a stand-alone installation package. Kaspersky Security Center Linux does not support installation of all Kaspersky applications.

## Local installation of Network Agent

*To install Network Agent on a device locally:*

1. On the device, run the setup.exe file from the distribution package downloaded from the internet.  
A window opens prompting you to select Kaspersky applications to install.
2. In the application selection window, click the **Install only Kaspersky Security Center 15 Network Agent** link to start the Network Agent setup wizard. Follow the instructions of the wizard.  
While the installation wizard is running, you can specify the advanced settings of Network Agent (see below).
3. If you want to use your device as the connection gateway for a specific administration group, in the **Connection gateway** window of the setup wizard select **Use Network Agent as a connection gateway in DMZ**.
4. To configure Network Agent during installation on a virtual machine:
  - a. If you plan to create dynamic virtual machines from the virtual machine image, enable dynamic mode of Network Agent for Virtual Desktop Infrastructure (VDI). To do this, in the **Advanced Settings** window of the setup wizard, select the **Enable dynamic mode for VDI** option.  
Skip this step if you do not plan to create dynamic virtual machines from the virtual machine image.
  - b. Optimize the Network Agent operation for VDI. To do this, in the **Advanced Settings** window of the setup wizard, select the **Optimize settings for VDI** option.  
Scanning of executable files for vulnerabilities at the device startup will be disabled. Also, this disables the sending of information about the following objects to Administration Server:
    - Hardware registry
    - Applications installed on the device
    - Microsoft Windows updates that must be installed on the local client device
    - Software vulnerabilities detected on the local client device

Furthermore, you will be able to enable the sending of this information in the Network Agent properties or in the Network Agent policy settings.

When the setup wizard finishes, Network Agent will be installed on the device.

You can view the properties of the Network Agent service; you can also start, stop, and monitor Network Agent activity by means of standard Microsoft Windows tools: Computer Management\Services.

## Installing Network Agent in silent mode

Network Agent can be installed in silent mode, that is, without the interactive input of installation parameters. Silent installation uses a Windows Installer package (MSI) for Network Agent. The MSI file is located in the Kaspersky Security Center Linux distribution package, in the Packages\NetAgent\exec folder.

*To install Network Agent on a local device in silent mode:*

1. Read the [End User License Agreement](#). Use the command below only if you understand and accept the terms of the End User License Agreement.

2. Run the command

```
msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters >
```

where `setup_parameters` is a list of parameters and their respective values, separated by a space (PROP1=PROP1VAL PROP2=PROP2VAL).

In the list of parameters, you must include `EULA=1`. Otherwise Network Agent will not be installed.

If you are using the standard connection settings for Kaspersky Security Center 11 and later, and Network Agent on remote devices, run the command:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` is the key for writing logs. The log is created during the installation of Network Agent and saved at `C:\windows\temp\nag_inst.log`.

In addition to `nag_inst.log`, the application creates the `$klssinstlib.log` file, which contains the installation log. This file is stored in the `%windir%\temp` or `%temp%` folder. For troubleshooting purposes, you or a Kaspersky Technical Support specialist may need both log files—`nag_inst.log` and `$klssinstlib.log`.

If you need to additionally specify the port for connection to the Administration Server run the command:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

The parameter `SERVERPORT` corresponds to the number of port for connection to Administration Server.

The names and possible values for parameters that can be used when installing Network Agent in silent mode are listed in the [Network Agent installation parameters](#) section.

## Local installation of the application management plug-in

*To install the application management plug-in:*

On a device with Administration Console installed, run the `klcfginst.exe` executable file, which is included in the application distribution package.

The `klcfginst.exe` file is included in all applications that can be managed through Kaspersky Security Center Linux. Installation is facilitated by the wizard and requires no manual configuration of settings.

## Installing applications in silent mode

To install an application in silent mode:

1. Open the main window of Kaspersky Security Center.
2. In the **Remote installation** folder of the console tree, in the **Installation packages** subfolder select the installation package of the relevant application or create a new one for that application.

The installation package will be stored on the Administration Server in the Packages service folder that is in the shared folder. A separate subfolder corresponds to each installation package.

3. Open the folder storing the required installation package in one of the following ways:
  - By copying the folder corresponding to the relevant installation package from the Administration Server to the client device. Then open the copied folder on the client device.
  - By opening from the client device the shared folder that corresponds to the requisite installation package on the Administration Server.

If the shared folder is located on a device that has Microsoft Windows Vista installed, you must set the **Disabled** value for the **User account control: Run all administrators in Admin Approval Mode** setting (**Start** → **Control Panel** → **Administration** → **Local security policy** → **Security settings**).

4. Depending on the selected application, do the following:
  - For Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers, and Kaspersky Security Center, navigate to the exec subfolder and run the executable file (the file with the .exe extension) with the /s key.
  - For other Kaspersky applications, run the executable file (a file with the .exe extension) with the /s key from the open folder.

Running the executable file with the EULA=1 and PRIVACYPOLICY=1 keys means that you have fully read, understand and accept the terms of the [End User License Agreement](#) and the [Privacy Policy](#), respectively. You are also aware that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy. The text of the License Agreement and the Privacy Policy is included in the Kaspersky Security Center Linux distribution kit. Accepting the terms of the License Agreement and the Privacy Policy is necessary for installing the application or upgrading a previous version of the application.

## Installing applications by using stand-alone packages

Kaspersky Security Center lets you create stand-alone installation packages for applications. A stand-alone installation package is an executable file that can be located on the Web Server, sent by email, or transferred to a client device by another method. The received file can be run locally on the client device to install an application without involving Kaspersky Security Center.

*To install an application using a stand-alone installation package:*

1. Connect to the necessary Administration Server.
2. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.
3. In the workspace, select the installation package of the required application.
4. Start the process of creating a stand-alone installation package in one of the following ways:
  - By selecting **Create stand-alone installation package** in the context menu of the installation package.
  - By clicking the **Create stand-alone installation package** link in the workspace of the installation package.

The Stand-alone installation package creation wizard starts. Follow the instructions of the wizard.

At the final step of the wizard, select a method for transferring the stand-alone installation package to the client device.

5. Transfer the stand-alone installation package to the client device.
6. Run the stand-alone installation package on the client device.

The application is now installed on the client device with the settings specified in the stand-alone package.

When you create a stand-alone installation package, it is automatically published on Web Server. The link for downloading the stand-alone package is displayed in the list of created stand-alone installation packages. If necessary, you can cancel publication of the selected stand-alone package and republish it on the Web Server. By default, port 8060 is used for downloading stand-alone installation packages.

## Network Agent installation package settings

*To configure a Network Agent installation package:*

1. In the **Remote installation** folder of the console tree, select the **Installation packages** subfolder.  
The **Remote installation** folder is a subfolder of the **Advanced** folder by default.
2. In the context menu of the Network Agent installation package, select **Properties**.

The Network Agent installation package properties window opens.

### General

The **General** section displays general information about the installation package:

- Installation package name
- Name and version of the application for which the installation package has been created
- Installation package size
- Installation package creation date

- Path to the installation package folder

## Settings

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](#) 

Status of the password: **Password set** or **Password not set**.

By default, this password is not installed.

- [Protect Network Agent service against unauthorized removal or termination, and prevent changes to the settings](#) 

When this option is enabled, after Network Agent is installed on a managed device, the component cannot be removed or reconfigured without required privileges. The Network Agent service cannot be stopped. This option has no effect on domain controllers.

Enable this option to protect Network Agent on workstations operated with local administrator rights.

By default, this option is disabled.

- [Automatically install applicable updates and patches for components that have the Undefined status](#) 

If this option is enabled, all downloaded updates and patches for Administration Server, Network Agent, Kaspersky Security Center Web Console, Exchange Mobile Device Server, and iOS MDM Server will be installed automatically.

If this option is disabled, all downloaded updates and patches will only be installed after you change their status to *Approved*. Updates and patches with *Undefined* status will not be installed.

By default, this option is enabled.

## Connection

In this section, you can configure connection of Network Agent to the Administration Server. To establish a connection, you can use the SSL or UDP protocol. For configuring the connection, specify the following settings:

- [Administration Server](#) 

Address of the device with Administration Server installed.

- [Port](#) 

Port number that is used for connection.

- [SSL port](#) 

Port number that is used for connection over the SSL protocol.

- [Use Server certificate](#) 

If this option is enabled, authentication of Network Agent access to the Administration Server will use the certificate file that you can specify by clicking the **Browse** button.

If this option is disabled, the certificate file will be received from the Administration Server at the first connection of Network Agent to the address specified in the **Server address** field.

We do not recommend to disable this option, because automatic receipt of an Administration Server certificate by Network Agent upon connection to the Administration Server is considered insecure.

By default, this check box is selected.

- [Use SSL](#) 

If this option is enabled, connection to the Administration Server is established through a secure port via SSL.

By default, this option is disabled. We recommend that you do not disable this option so your connection remains secured.

- [Use UDP port](#) 



If this option is enabled, the Network Agent is connected to Administration Server through a UDP port. This allows to manage client devices and receive information about them.

The UDP port must be open on managed devices where Network Agent is installed. Therefore, we recommend that you do not disable this option.

By default, this option is enabled.

- [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, UDP ports used by Network Agent are added to the Microsoft Windows Firewall exclusion list.

By default, this option is enabled.

- [Use proxy server](#) 

If this option is disabled, direct connection is used to connect the device to the Administration server.

If this option is enabled, specify the proxy server parameters:


- **Proxy server address**
- **Proxy server port**

If your proxy server requires authentication, enable the **Proxy server authentication** option and specify the **User name** and **Password** of the account under which connection to the proxy server is established. We recommend that you specify the credentials of an account that has minimum privileges required only for the proxy server authentication.

For compatibility purposes, it is not recommended to specify proxy connection settings in the Network Agent installation package settings.

## Advanced

In the **Advanced** section, you can configure how to use the connection gateway. For this purpose, you can do the following:

- Use Network Agent as a connection gateway in the demilitarized zone (DMZ) to connect to Administration Server, communicate with it, and [keep data on the Network Agent safe](#) during data transmission.
- Connect to Administration Server by using a connection gateway to reduce the number of connections to the Administration Server. In this case, enter the address of the device that will act as the connection gateway in the **Connection gateway address** field.
- Configure the connection for Virtual Desktop Infrastructure (VDI) if your network includes virtual machines. For this purpose, do the following:
  - [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.

## 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         | ✓       | —                                                                                                                                                    | —                                                                                                                                                    |
| Connection       | ✓       | ✓<br>(except for the <b>Open Network Agent ports in Microsoft Windows Firewall</b> and <b>Use only automatic detection of proxy server options</b> ) | ✓<br>(except for the <b>Open Network Agent ports in Microsoft Windows Firewall</b> and <b>Use only automatic detection of proxy server options</b> ) |

|                       |   |                                               |                                               |
|-----------------------|---|-----------------------------------------------|-----------------------------------------------|
| Advanced              | ✓ | ✓                                             | ✓                                             |
| Additional components | ✓ | ✓                                             | ✓                                             |
| Tags                  | ✓ | ✓<br>(except for the automatic tagging rules) | ✓<br>(except for the automatic tagging rules) |
| Revision history      | ✓ | ✓                                             | ✓                                             |

## Manual setup of the group task for scanning a device with Kaspersky Endpoint Security

The [quick start wizard](#) creates a group task for scanning a device. If the automatically specified schedule of the group scanning task is not appropriate for your organization, you must manually set up the most convenient schedule for this task based on the workplace rules adopted in the organization.

For example, the task is assigned a **Run on Fridays at 7:00 PM** schedule with automatic randomization, and the **Run missed tasks** check box is cleared. This means that if the devices in the organization are shut down on Fridays, for example, at 6:30 PM, the device scan task will never run. In this case you need to set up the group scanning task manually.

# Managing client devices

This section describes how to manage devices in the administration groups.

## Settings of a managed device

*To view the settings of a managed device:*

1. In the main menu, go to **Assets (Devices)** → **Managed devices**.

The list of managed devices is displayed.

2. In the list of managed devices, click the link with the name of the required device.

The properties window of the selected device is displayed.

The following tabs are displayed in the upper part of the properties window representing the main groups of the settings:

- [General](#) 

This tab comprises the following sections:

- The **General** section displays general information about the client device. Information is provided on the basis of data received during the last synchronization of the client device with the Administration Server:

- **[Name](#)**

In this field, you can view and modify the client device name in the administration group.

- **[Description](#)**

In this field, you can enter an additional description for the client device.

- **[Device status](#)**

Status of the client device assigned on the basis of the criteria defined by the administrator for the status of anti-virus protection on the device and the activity of the device on the network.

- **[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.

- **[Full group name](#)**

Administration group, which includes the client device.

- **[Last update of anti-virus databases](#)**

Date the anti-virus databases or applications were last updated on the device.

- **[Connected to Administration Server](#)**

Date and time Network Agent installed on the client device last connected to the Administration Server.

- **[Last visible](#)**

Date and time the device was last visible on the network.

- **[Network Agent version](#)**

Version of the installed Network Agent.

- **[Created](#)**

Date of the device creation within Kaspersky Security Center Linux.

- [Do not disconnect from the Administration Server](#) 

If this option is enabled, continuous connectivity between the managed device and the Administration Server is maintained. You may want to use this option if you are not using push servers, which provide such connectivity.

If this option is disabled and push servers are not in use, the managed device only connects to the Administration Server to synchronize data or to transmit information.

The maximum total number of devices with the **Do not disconnect from the Administration Server** option selected is 300.

This option is disabled by default on managed devices. This option is enabled by default on the device where the Administration Server is installed and stays enabled even if you try to disable it.

- The **Network** section displays the following information about the network properties of the client device:

- [IP address](#) 

Device IP address.

- [Windows domain](#) 

Workgroup that contains the device.

- [DNS name](#) 

Name of the DNS domain of the client device.

- [NetBIOS name](#) 

Name of the client device.

- **IPv6 address**

- The **System** section provides information about the operating system installed on the client device:

- **Operating system**

- **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 anti-virus application (first scan), or since the last reset of the threat counter.

- [Objects that have failed disinfection](#) 

Number of unprocessed files on the client device.

This field ignores the number of unprocessed files on mobile devices.

- [Disk encryption status](#) 

The current status of file encryption on the local drives of the device. For a description of the statuses, see the [Kaspersky Endpoint Security for Windows Help](#) .

Files can be only encrypted on the managed devices on which Kaspersky Endpoint Security for Windows is installed.

- The **Device status defined by application** section provides information about the device status that is defined by the managed application installed on the device. This device status can differ from the one defined by Kaspersky Security Center Linux.

- [Applications](#) 

This tab lists all Kaspersky applications installed on the client device. 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 which are currently active on the managed device.

- [Tasks](#) 

In 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 connection is not established, the status is not displayed.

- [Events](#) 

The **Events** tab displays events logged on the Administration Server for the selected client device.

- [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.

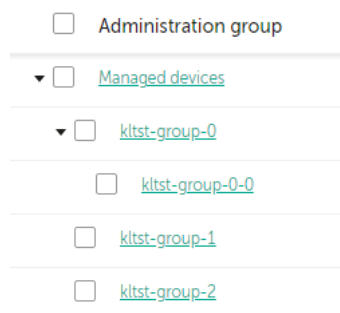
- [Properties](#) 

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.
- **Remote diagnostics.** In this section, you can perform [remote diagnostics of client devices](#).

## Creating administration groups

Immediately after Kaspersky Security Center installation, the hierarchy of administration groups contains only one administration group called **Managed devices**. When creating a hierarchy of administration groups, you can add devices and virtual machines to the **Managed devices** group, and add nested groups (see the figure below).



Viewing administration groups hierarchy

*To create an administration group:*

1. In the main menu, go to **Assets (Devices)** → **Hierarchy of groups**.

2. In the administration group structure, select the administration group that is to include the new administration group.
3. Click the **Add** button.
4. In the **Name of the new administration group** window that opens, enter a name for the group, and then click the **Add** button.

A new administration group with the specified name appears in the hierarchy of administration groups.

*To create a structure of administration groups:*

1. In the main menu, go to **Assets (Devices) → Hierarchy of groups**.
2. Click the **Import** button.

The New Administration Group Structure Wizard starts. Follow the instructions of the Wizard.

## Device moving rules

We recommend that you automate the allocation of devices to administration groups through *device moving rules*. A device moving rule consists of three main parts: a name, an [execution condition](#) (logical expression with the device attributes), and a target administration group. A rule moves a device to the target administration group if the device attributes meet the rule execution condition.

All device moving rules have priorities. The Administration Server checks the device attributes as to whether they meet the execution condition of each rule, in ascending order of priority. If the device attributes meet the execution condition of a rule, the device is moved to the target group, so the rule processing is complete for this device. If the device attributes meet the conditions of multiple rules, the device is moved to the target group of the rule with the highest priority (that is, has the highest rank in the list of rules).

Device moving rules can be created implicitly. For example, in the properties of an installation package or a remote installation task, you can specify the administration group to which the device must be moved after Network Agent is installed on it. Also, device moving rules can be created explicitly by the administrator of Kaspersky Security Center Linux, in the **Assets (Devices) → Moving rules** section.

By default, a device moving rule is intended for one-time initial allocation of devices to administration groups. The rule moves devices from the unassigned devices group only once. If a device once was moved by this rule, the rule will never move it again, even if you return the device to the unassigned devices group manually. This is the recommended way of applying moving rules.

You can move devices that have already been allocated to some of the administration groups. To do this, in the properties of a rule, clear the **Move only devices that do not belong to an administration group** check box.

Applying moving rules to devices that have already been allocated to some of the administration groups, significantly increases the load on the Administration Server.

The **Move only devices that do not belong to an administration group** check box is locked in the properties of automatically created moving rules. Such rules are created when you add the *Install application remotely* task or create a stand-alone installation package.

You can create a moving rule that would affect a single device repeatedly.

We strongly recommend that you avoid moving a single device from one group to another repeatedly (for example, in order to apply a special policy to that device, run a special group task, or update the device through a specific distribution point).

Such scenarios are not supported, because they increase the load on Administration Server and network traffic to an extreme degree. These scenarios also conflict with the operating principles of Kaspersky Security Center Linux (particularly in the area of access rights, events, and reports). Another solution must be found, for example, through the use of policy profiles, tasks for [device selections](#), assignment of [Network Agents according to the standard scenario](#), and so on.

## 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 **Assets (Devices)** → **Moving rules**.
2. Click **Add**.
3. In the window that opens, specify the following information on the **General** tab:

- [Rule name](#) ⓘ

Enter a name for the new rule.

If you are copying a rule, the new rule gets the same name as the source rule, but an index in () format is added to the name, for example: (1).

- [Administration group](#) ⓘ

Select the administration group into which the devices are to be moved automatically.

- [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.

- [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 increase or decrease the priority of a moving rule, move the rule up or down in the list, respectively, using the mouse.

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 **Assets (Devices) → 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.

- [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.

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:

- [DNS name of the device](#) 

DNS domain name of the client device that you want to move. Fill this field if your network includes a DNS server.

If case sensitive collation is set for the database that you use for Kaspersky Security Center Linux, keep case when you specify a device DNS name. Otherwise, the device moving rule will not work.

- [DNS domain](#) 

A device moving rule applies to all devices included in the specified main DNS suffix. Fill this field if your network includes a DNS server.

- [IP range](#) 

If this option is enabled, you can enter the initial and final IP addresses of the IP range in which the relevant devices must be included.

By default, this option is disabled.

- [IP address for connection to Administration Server](#) 

If this option is enabled, you can set the IP addresses by which client devices are connected to Administration Server. To do this, specify the IP range that includes all necessary IP addresses.

By default, this option is disabled.

- [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 15 Network Agent** or **Kaspersky Security Center 15 Administration Server**.

If you do not select any managed application, the condition does not apply.

- [Operating system version](#) 

You can cull client devices based on the operating system version. For this purpose, specify operating systems that should be installed on the client devices. As a result, a device moving rule applies to the client devices with the selected operating systems.


If you do not enable this option, the condition does not apply. By default, the option is disabled.

- [Operating system bit size](#) 

You can cull client devices by the operating system bit sizes. In the **Operating system bit size** 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 **Assets (Devices)** → **Managed devices** section.
2. Click the **Columns settings** button (  ) on the right.
3. Select the **Operating system bit size** option, and then click the **Save** button.

After that, the operating system bit size is displayed for every managed device.

- [Operating system 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.

- [Operating system build](#) 



This setting is applicable to Windows operating systems only.

You can specify whether the selected operating system must have an equal, earlier, or later build number. You can also configure a device moving rule for all build numbers except the specified one.

- [Operating system release number](#) 

This setting is applicable to Windows operating systems only.

You can specify whether the selected operating system must have an equal, earlier, or later release number. You can also configure a device moving rule for all release numbers except the specified one.

## Virtual machines tab

On this tab, you can configure a device moving rule according to whether client devices are virtual machines or part of a virtual desktop infrastructure (VDI):

- [This is a virtual machine](#) 

In the drop-down list, you can select one of the following:

- **N/A.** The condition does not apply.
- **No.** Move devices that are not virtual machines.
- **Yes.** Move devices that are virtual machines.

- **Virtual machine type**

- [Part of Virtual Desktop Infrastructure](#) 

In the drop-down list, you can select one of the following:

- **N/A.** The condition does not apply.
- **No.** Move devices that are not part of VDI.
- **Yes.** Move devices that are part of VDI.

## Domain controller tab

On this tab, you can specify that it is necessary to move devices included in the domain organizational unit. You can also move devices from all child organizational units of the specified domain organizational unit:

- [Device is included in the following organizational unit](#) 


If this option is enabled, a device moving rule applies to devices from the domain controller organizational unit specified in the list under the option.

By default, this option is disabled.

- [Include child organizational units](#) 

If this option is enabled, the selection includes devices from all child organizational units of the specified domain controller organizational unit.

By default, this option is disabled.

- **Move devices from child units to corresponding subgroups**
- **Create subgroups corresponding to containers of newly detected devices**
- **Delete subgroups that are not present in the domain**
- [Device is included in the following domain security group](#) 

If this option is enabled, a device moving rule applies to devices from the domain security group specified in the list under the option.

By default, this option is disabled.

## 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 **Assets (Devices)** → **Managed devices**.
2. Click the **Current path:** <current path> link above the list.
3. In the window that opens, select the administration group to which you want to add the devices.
4. Click the **Add devices** button.  
The Move devices wizard starts.
5. 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.
- Specify a device DNS name.

The device name field must not contain space characters, backspace characters, or the following prohibited characters: , \ / \* ' " ; : & ` ~ ! @ # \$ ^ ( ) = + [ ] { } | < > %

- Click the **Import devices from file** button to import a list of devices from a .txt file. Each device address or name must be specified on a separate line.

The file must not contain space characters, backspace characters, or the following prohibited characters: , \ / \* ' " ; : & ` ~ ! @ # \$ ^ ( ) = + [ ] { } | < > %

6. View the list of devices to be added to the administration group. You can edit the list by adding or removing devices.

7. 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 this, perform one of the following:
  - To open an administration group, in the main menu, go to **Assets (Devices)** → **Managed devices**, click the path link in the **Current path** field, and select an administration group in the left-side pane that opens.
  - 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 **Managed devices** section is divided into two tabs—the **Devices** tab and the **Clusters and server arrays** tab. Open the tab for the object that you want to move.
3. Select the check boxes next to the devices or clusters that you want to move to a different group.

4. Click the **Move to group** button.
5. In the hierarchy of administration groups, select the check box next to the administration group to which you want to move the selected devices or clusters.
6. Click the **Move** button.

The selected devices or clusters are moved to the selected administration group.

## About clusters and server arrays

Kaspersky Security Center Linux supports cluster technology. If Network Agent sends information to Administration Server confirming that an application installed on a client device is part of a server array, this client device becomes a cluster node.

If an administration group contains clusters or server arrays, the **Managed devices** page displays two tabs—one for individual devices, and one for clusters and server arrays. After the managed devices are detected as cluster nodes, the cluster is added as an individual object to the **Clusters and server arrays** tab.

The cluster or server array nodes are listed on the **Devices** tab, along with other managed devices. You can [view properties](#) of the nodes as individual devices and perform other operations, but you cannot delete a cluster node or move it to another administration group separately from its cluster. You can only delete or move an entire cluster.

You can perform the following operations with clusters or server arrays:

- [View properties](#)
- [Move the cluster or server array to another administration group](#)

When you move a cluster or server array to another group, all of its nodes move with it, because a cluster and any of its nodes always belong to the same administration group.
- Delete

It is reasonable to delete a cluster or server array only when the cluster or server array does not exist in the organization network any longer. If a cluster is still visible on your network and Network Agent and the Kaspersky security application are still installed on the cluster nodes, Kaspersky Security Center Linux returns the deleted cluster and its nodes back to the list of managed devices automatically.

## Properties of a cluster or server array

*To view the settings of a cluster or server array:*

1. In the main menu, go to **Assets (Devices)** → **Managed devices** → **Clusters and server arrays**.


The list of clusters and server arrays is displayed.

2. Click the name of the required cluster or server array.

The properties window of the selected cluster or server array is displayed.

## General

The **General** section displays general information about the cluster or server array. Information is provided on the basis of data received during the last synchronization of the cluster nodes with the Administration Server:

- **Name**
- **Description**
- **[Windows domain](#)** 

Windows domain or workgroup, which contains the cluster or server array.

- **[NetBIOS name](#)** 

Windows network name of the cluster or server array.

- **[DNS name](#)** 

Name of the DNS domain of the cluster or server array.

## Tasks

In the **Tasks** tab, you can manage the tasks assigned to the cluster or server array: view the list of existing tasks; create new ones; remove, start, and stop tasks; modify task settings; and view execution results. The listed tasks relate to the Kaspersky security application installed on the cluster nodes. Kaspersky Security Center Linux receives the task list and the task status details from the cluster nodes. If a connection is not established, the status is not displayed.

## Nodes

This tab displays a list of nodes included into the cluster or server array. You can click a node name to view the [device properties window](#).

## Kaspersky application

The properties window may also contain additional tabs with the information and settings related to the Kaspersky security application installed on the cluster nodes.

## Adjustment of distribution points and connection gateways

A structure of administration groups in Kaspersky Security Center Linux performs the following functions:

- Sets the scope of policies  
There is an alternate way of applying relevant settings on devices, by using *policy profiles*.
- Sets the scope of group tasks

There is an approach to defining the scope of group tasks that is not based on a hierarchy of administration groups: use of tasks for device selections and tasks for specific devices.

- Sets access rights to devices, virtual Administration Servers, and secondary Administration Servers
- Assigns distribution points

When building the structure of administration groups, you must take into account the topology of the organization's network for the optimum assignment of distribution points. The optimum distribution of distribution points allows you to save traffic on the organization's network.

Depending on the organizational schema and network topology, the following standard configurations can be applied to the structure of administration groups:

- Single office
- Multiple small remote offices

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

## Standard configuration of distribution points: Single office

In a standard "single-office" configuration, all devices are on the organization's network so they can "see" each other. The organization's network may consist of a few separate parts (networks or network segments) linked by narrow channels.

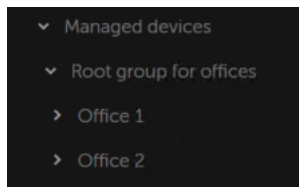
The following methods of building the structure of administration groups are possible:

- Building the structure of administration groups taking into account the network topology. The structure of administration groups may not reflect the network topology with absolute precision. A match between the separate parts of the network and certain administration groups would be enough. You can use automatic assignment of distribution points or assign them manually.
- Building the structure of administration groups, without taking the network topology into account. In this case, you must disable automatic assignment of distribution points, and then assign one or several devices to act as distribution points for a root administration group in each of the separate parts of the network, for example, for the **Managed devices** group. All distribution points will be at the same level and will feature the same scope spanning all devices on the organization's network. In this case, each Network Agent will connect to the distribution point that has the shortest route. The route to a distribution point can be traced with the `tracert` utility.

## Standard configuration of distribution points: Multiple small remote offices

This standard configuration provides for a number of small remote offices, which may communicate with the head office over the internet. Each remote office is located behind the NAT, that is, connection from one remote office to another is not possible because offices are isolated from one another.

The configuration must be reflected in the structure of administration groups: a separate administration group must be created for each remote office (groups **Office 1** and **Office 2** in the figure below).



Remote offices are included in the administration group structure

One or multiple distribution points must be assigned to each administration group that correspond to an office. Distribution points must be devices at the remote office that have a [sufficient amount of free disk space](#). Devices deployed in the **Office 1** group, for example, will access distribution points assigned to the **Office 1** administration group.

If some users move between offices physically, with their laptops, you must select two or more devices (in addition to the existing distribution points) in each remote office and assign them to act as distribution points for a top-level administration group (**Root group for offices** in the figure above).

Example: A laptop is deployed in the **Office 1** administration group and then is moved physically to the office that corresponds to the **Office 2** administration group. After the laptop is moved, Network Agent attempts to access the distribution points assigned to the **Office 1** group, but those distribution points are unavailable. Then, Network Agent starts attempting to access the distribution points that have been assigned to the **Root group for offices**. Because remote offices are isolated from one another, attempts to access distribution points assigned to the **Root group for offices** administration group will only be successful when Network Agent attempts to access distribution points in the **Office 2** group. That is, the laptop will remain in the administration group that corresponds to the initial office, but the laptop will use the distribution point of the office where it is physically located at the moment.

## Calculating the number and configuration of distribution points

The more client devices a network contains, the more distribution points it requires. We recommend that you not disable automatic assignment of distribution points. When automatic assignment of distribution points is enabled, Administration Server assigns distribution points if the number of client devices is quite large and defines their configuration.

### Using exclusively assigned distribution points

If you plan to use certain specific devices as distribution points (that is, exclusively assigned servers), you can opt out of using automatic assignment of distribution points. In this case, make sure that the devices that you intend to make distribution points have sufficient volume of [free disk space](#), are not shut down regularly, and have Sleep mode disabled.

Number of exclusively assigned distribution points on a network that contains a single network segment, based on the number of networked devices

| Number of client devices in the 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 exclusively assigned 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) |

|               |                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------|
| 10–100        | 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 in the network segment | Number of distribution points                                                                            |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Less than 300                                   | 0 (Do not assign distribution points)                                                                    |
| More than 300                                   | $(N/300 + 1)$ , where N is the number of networked devices; there must be at least 3 distribution points |

Number of workstations functioning as distribution points on a network that contains multiple network segments, based on the number of networked devices

| Number of client devices per network segment | Number of distribution points                                                                            |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Less than 10                                 | 0 (Do not assign distribution points)                                                                    |
| 10–30                                        | 1                                                                                                        |
| 31–300                                       | 2                                                                                                        |
| More than 300                                | $(N/300 + 1)$ , where N is the number of networked devices; there must be at least 3 distribution points |

If a distribution point is shut down (or not available for some other reason), the managed devices in its scope can access the Administration Server for updates.

## Assigning distribution points automatically

We recommend that you assign distribution points automatically. In this case, Kaspersky Security Center Linux will select on its own which devices must be assigned distribution points.

*To assign distribution points automatically:*

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 **Distribution points** section.
3. Select the **Automatically assign distribution points** option.

If automatic assignment of devices as distribution points is enabled, you cannot configure distribution points manually or edit the list of distribution points.



4. Click the **Save** button.

Administration Server assigns and configures distribution points automatically.

## Assigning distribution points manually

Kaspersky Security Center Linux allows you to manually assign devices to act as distribution points.

We recommend that you assign distribution points automatically. In this case, Kaspersky Security Center Linux will select on its own which devices must be assigned distribution points. However, if you have to opt out of assigning distribution points automatically for any reason (for example, if you want to use exclusively assigned servers), you can assign distribution points manually after you [calculate their number and configuration](#).

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 settings icon (⚙️) next to the name of the required Administration Server.  
The Administration Server properties window opens.
2. On the **General** tab, select the **Distribution points** section.
3. Select the **Manually assign distribution points** option.
4. Click the **Assign** button.
5. Select the device that you want to make a distribution point.  
When selecting a device, keep in mind the operation features of distribution points and the requirements set for the device that acts as distribution point.
6. Select the administration group that you want to include in the scope of the selected distribution point.
7. Click the **OK** button.  
The distribution point that you have added will be displayed in the list of distribution points, in the **Distribution points** section.
8. Click the newly added distribution point in the list to open its properties window.
9. Configure the distribution point in the properties window:
  - The **General** section contains the settings of interaction between the distribution point and client devices.

- **SSL port** ⓘ

The number of the SSL port for encrypted connection between client devices and the distribution point using SSL.

By default, port 13000 is used.

- [Use multicast](#) 

If this option is enabled, IP multicasting will be used for automatic distribution of installation packages to client devices within the group.

IP multicasting decreases the time required to install an application from an installation package to a group of client devices, but increases the installation time when you install an application to a single client device.

- [IP multicast address](#) 

IP address that will be used for multicasting. You can define an IP address in the range of 224.0.0.0 – 239.255.255.255

By default, Kaspersky Security Center Linux automatically assigns a unique IP multicast address within the given range.

- [IP multicast port number](#) 

Number of the port for IP multicasting.

By default, the port number is 15001. If the device with Administration Server installed is specified as the distribution point, port 13001 is used for SSL connection by default.

- [Distribution point address for remote devices](#) 

The IPv4 address through which remote devices connect to the distribution point.

- [Deploy updates](#) 

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 [calculate](#) 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, this option is enabled.

- [Deploy installation packages](#) 

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 [calculate](#) 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, this option is enabled.

- [Run push server](#) 

In Kaspersky Security Center Linux, a distribution point can work as a push server for the devices managed through the mobile protocol and for the devices managed by Network Agent. For example, a push server must be enabled if you want to be able to [force synchronization](#) of KasperskyOS devices with Administration Server. A push server has the same scope of managed devices as the distribution point on which the push server is enabled. If you have several distribution points assigned for the same administration group, you can enable push server on each of the distribution points. In this case, Administration Server balances the load between the distribution points.

- [Push server port](#) 

The port number for the push server. You can specify the number of any unoccupied port.

- In the **Scope** section, specify administration groups to which the distribution point will distribute updates.
- In the **Source of updates** section, you can select a source of updates for the distribution point:

- [Source of updates](#) 

Select a source of updates for the distribution point:

- To allow the distribution point to receive updates from the Administration Server, select **Retrieve from Administration Server**.
- To allow the distribution point to receive updates by using a task, select **Use update download task**, and then specify a *Download updates to the repositories of distribution points* task:
  - If such a task already exists on the device, select the task in the list.
  - If no such task yet exists on the device, click the **Create task** link to create a task. The New task wizard starts. Follow the instructions of the wizard.

- [Download diff files](#) 

This option enables the [downloading diff files feature](#).

By default, this option is enabled.

- In the **Internet connection settings** subsection, you can specify the internet access settings:

- [Use proxy server](#) 

If this check box is selected, in the entry fields you can configure the proxy server connection.  
By default, this check box is cleared.

- [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.  
By default, this check box is cleared.

- [User name](#) 

User account under which connection to the proxy server is established.

- [Password](#) 

Password of the account under which the task will be run.

- In the **KSN Proxy** section, you can configure the application to use the distribution point to forward KSN requests from the managed devices:

- [Enable KSN Proxy on the distribution point side](#) 

The KSN proxy service is run on the device that is used as a distribution point. Use this feature to redistribute and optimize traffic on the network.

The distribution point sends the KSN statistics, which are listed in the Kaspersky Security Network statement, to Kaspersky.

By default, this option is disabled. Enabling this option takes effect only if the **Use Administration Server as a proxy server** and **I agree to use Kaspersky Security Network** options are enabled in the Administration Server properties window.

You can assign a node of an active-passive cluster to a distribution point and enable KSN proxy server on this node.

- [Forward KSN requests to Administration Server](#) 

The distribution point forwards KSN requests from the managed devices to the Administration Server.

By default, this option is enabled.

- [Access KSN Cloud/KPSN directly over the internet](#) 

The distribution point forwards KSN requests from managed devices to the KSN Cloud or KPSN. The KSN requests generated on the distribution point itself are also sent directly to the KSN Cloud or KPSN.

- [Ignore proxy server settings when connecting to KPSN](#) 

Enable this option, if you have the proxy server settings configured in the distribution point properties or in the Network Agent policy, but your network architecture requires that you use KPSN directly. Otherwise, requests from the managed applications cannot reach KPSN.

This option is available if you select the **Access KSN Cloud/KPSN directly over the internet** option.

- [Port](#) 

The number of the TCP port that the managed devices will use to connect to KSN proxy server. The default port number is 13111.

- [Use UDP port](#) 

If you need the managed devices to connect to KSN proxy server through a UDP port, enable the **Use UDP port** option and specify a UDP port number. By default, this 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.

- In the **Connection gateway** section, you can configure the distribution point to act as a gateway for connection between Network Agent instances and Administration Server:

- [Connection gateway](#) 

If a direct connection between Administration Server and Network Agents cannot be established due to organization of your network, you can use the distribution point to act as the [connection gateway](#) between Administration Server and Network Agents.

Enable this option if you need the distribution point to act as a connection gateway between Network Agents and Administration Server. By default, this option is disabled.

- [Establish connection to gateway from Administration Server \(if gateway is in DMZ\)](#) 

If Administration Server is located outside the demilitarized zone (DMZ), on local area network, Network Agents installed on remote devices cannot connect to Administration Server. You can use a distribution point as the connection gateway with reverse connectivity (Administration Server establishes a connection to distribution point).

Enable this option if you need to connect Administration Server to the connection gateway in DMZ.

- [Open local port for Kaspersky Security Center Web Console](#) 

Enable this option if you need the connection gateway in DMZ to open a port for Web Console that is in DMZ or on the internet. Specify the port number that will be used for the connection from Web Console to the distribution point. The default port number is 13299.

This option is available if you enable the **Establish connection to gateway from Administration Server (if gateway is in DMZ)** option.

- [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. 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. Specify the following parameters:

- 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.

- Configure domain controller polling by the distribution point.

- [Domain controller polling](#) 

You can enable device discovery for domain controllers.

If you select the **Enable domain controller polling** option, 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.

If you use a Windows distribution point, you can select one of the following options:

- **Poll current domain**
- **Poll entire domain forest**
- **Poll specified domains**

- Configure the polling of IP ranges by the distribution point.

- [IP ranges polling](#) 

You can enable device discovery for IPv4 ranges and IPv6 networks.

If you enable the **Enable range polling** option, you can add scanned ranges and set the schedule for them. You can add IP ranges to the list of scanned ranges.

If you enable the **Use Zeroconf to poll IPv6 networks** option, the distribution point automatically polls the IPv6 network by using [zero-configuration networking](#) (also referred to as *Zeroconf*). In this case, the specified IP ranges are ignored because the distribution point polls the whole network. The **Use Zeroconf to poll IPv6 networks** option is available if the distribution point runs Linux. To use Zeroconf IPv6 polling, you must install the `avahi-browse` utility on the distribution point.

- In the **Advanced** section, specify the folder that the distribution point must use to store distributed data.

- [Use default folder](#) 

If you select this option, the application uses the Network Agent installation folder on the distribution point.

- [Use specified folder](#) 

If you select this option, in the field below, you can specify the path to the folder. It can be a local folder on the distribution point, or it can be a folder on any device on the corporate network.

The user account used on the distribution point to run Network Agent must have read/write access to the specified folder.

10. Click the **OK** button.

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 **Assets (Devices)** → **Managed devices**.
2. In the **Current path** field above the list of managed devices, click the path link.
3. In the left-side pane that opens, select an administration group for which you want to view the assigned distribution points.  
This enables the **Distribution points** menu item.
4. In the main menu, go to **Assets (Devices)** → **Distribution points**.
5. To add new distribution points for the administration group, click the **Assign** button.
6. To remove the assigned distribution points, select devices from the list and click the **Unassign** button.

Depending on your modifications, the new distribution points are added to the list or existing distribution points are removed from the list.

## Enabling a push server

In Kaspersky Security Center Linux, a distribution point can work as a push server for the devices managed through the mobile protocol and for the devices managed by Network Agent. For example, a push server must be enabled if you want to be able to [force synchronization](#) of KasperskyOS devices with Administration Server. A push server has the same scope of managed devices as the distribution point on which the push server is enabled. If you have several distribution points assigned for the same administration group, you can enable push server on each of the distribution points. In this case, Administration Server balances the load between the distribution points.

You might want to use distribution points as push servers to make sure that there is continuous connectivity between a managed device and the Administration Server. Continuous connectivity is needed for some operations, such as running and stopping local tasks, receiving statistics for a managed application, or creating a tunnel. If you use a distribution point as a push server, you do not have to use the **Do not disconnect from the Administration Server** option on managed devices or send packets to the UDP port of the Network Agent.

A push server supports the load of up to 50,000 simultaneous connections.

*To enable push server on a distribution point:*

1. In the main menu, click the settings icon (⚙️) next to the name of the required Administration Server.  
The Administration Server properties window opens.
2. On the **General** tab, select the **Distribution points** section.
3. Click the name of the distribution point on which you want to enable the push server.  
The distribution point properties window opens.
4. On the **General** section, enable the **Run push server** option.
5. In the **Push server port** field, type the port number. You can specify number of any unoccupied port.



6. In the **Address for remote hosts** field, specify the IP address or the name of the distribution point device.

7. Click the **OK** button.

The push server is enabled on the selected distribution point.

## About device statuses

Kaspersky Security Center Linux assigns a status to each managed device. The particular status depends on whether the conditions defined by the user are met. In some cases, when assigning a status to a device, Kaspersky Security Center Linux takes into consideration the device's visibility flag on the network (see the table below). If Kaspersky Security Center Linux does not find a device on the network within two hours, the visibility flag of the device is set to *Not Visible*.

The statuses are the following:

- *Critical* or *Critical/Visible*
- *Warning* or *Warning/Visible*
- *OK* or *OK/Visible*

The table below lists the default conditions that must be met to assign the *Critical* or *Warning* status to a device, with all possible values.

Conditions for assigning a status to a device

| Condition                                                                  | Condition description                                                                                                                                                                                                                                                                                                                | Available values                                                                                       |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Security application is not installed                                      | Network Agent is installed on the device, but a security application is not installed.                                                                                                                                                                                                                                               | <ul style="list-style-type: none"><li>• Toggle button is on.</li><li>• Toggle button is off.</li></ul> |
| Too many viruses detected                                                  | Some viruses have been found on the device by a task for virus detection, for example, the Malware scan task, and the number of viruses found exceeds the specified value.                                                                                                                                                           | More than 0.                                                                                           |
| Real-time protection level differs from the level set by the Administrator | The device is visible on the network, but the real-time protection level differs from the level set (in the condition) by the administrator for the device status.                                                                                                                                                                   | <ul style="list-style-type: none"><li>• Stopped.</li><li>• Paused.</li><li>• Running.</li></ul>        |
| 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 <i>Malware scan</i> 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                                                                  | The device is visible on the network and a security application is installed                                                                                                                                                                                                                                                         | More than 1                                                                                            |

|                                         |                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                          |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| are outdated                            | 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. | 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 <b>Active threats</b> 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.                                                                                 | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                                                                                                                                                                                |
| License expired                         | The device is visible on the network, but the license has expired.                                                                                                                                                                           | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                                                                                                                                                                                |
| License expires soon                    | The device is visible on the network, but the license will expire on the device in less than the specified number of days.                                                                                                                   | More than 0 days.                                                                                                                                                                                                                                                                        |
| Invalid encryption status               | Network Agent is installed on the device, but the device encryption result is equal to the specified value.                                                                                                                                  | <ul style="list-style-type: none"> <li>• Does not comply with the policy due to the user's refusal (for external devices only).</li> <li>• Does not comply with the policy due to an error.</li> <li>• Restart is required when applying the policy.</li> <li>• No encryption</li> </ul> |

|                                      |                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                     |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                                      |                                                                                                                                                                                                                                                                                                                                                                                  | <p>policy is specified.</p> <ul style="list-style-type: none"> <li>• Not supported.</li> <li>• When applying the policy.</li> </ul> |
| 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.                                                                                                                                                    | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                           |
| Device status defined by application | The status of the device is defined by the managed application.                                                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                           |
| 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 <i>Critical</i> or <i>Warning</i> status is changed to the <i>OK</i> 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.                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                           |
| Protection is disabled               | <p>The device is visible on the network, but the security application on the device has been disabled for longer than the specified time interval.</p> <p>In this case, the state of the security application is <i>stopped</i> or <i>failure</i>, and differs from the following: <i>starting</i>, <i>running</i>, or <i>suspended</i>.</p>                                     | 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.                                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                           |

Kaspersky Security Center Linux allows you to set up automatic switching of the status of a device in an administration group when specified conditions are met. When the specified conditions are met, the client device is assigned one of the following statuses: *Critical* or *Warning*. When the specified conditions are not met, the client device is assigned the *OK* status.

Different statuses may correspond to different values of one condition. For example, by default, if the **Databases are outdated** condition has the **More than 3 days** value, the client device is assigned the *Warning* status; if the value is **More than 7 days**, the *Critical* status is assigned.

If you upgrade Kaspersky Security Center Linux from the previous version, the values of the **Databases are outdated** condition for assigning the status to *Critical* or *Warning* do not change.

When Kaspersky Security Center Linux 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. Open the properties window in one of the following ways:
  - In the **Policies** folder, in the context menu of an Administration Server policy, select **Properties**.
  - Select **Properties** in the context menu of an administration group.
2. In the **Properties** window that opens, in the **Sections** pane, select **Device status**.
3. In the right pane, in the **Set to Critical if these are specified** section, select the check box next to a condition in the list.

You can change only settings that are not locked in the parent policy.

4. Set the required value for the selected condition.  
You can set values for some, but not all, conditions.
5. Click **OK**.

When specified conditions are met, the managed device is assigned the *Critical* status.

*To enable changing the device status to Warning:*

1. Open the properties window in one of the following ways:
  - In the **Policies** folder, in the context menu of the Administration Server policy, select **Properties**.
  - Select **Properties** in the context menu of the administration group.
2. In the **Properties** window that opens, in the **Sections** pane select **Device status**.
3. In the right pane, in the **Set to Warning if these are specified** section, select the check box next to a condition in the list.

You can change only settings that are not locked in the parent policy.

4. Set the required value for the selected condition.

You can set values for some, but not all, conditions.

5. Click **OK**.

When specified conditions are met, the managed device is assigned the *Warning* status.

## Device selections

*Device selections* are a tool for filtering devices according to specific conditions. You can use device selections to manage several devices: for example, to view a report about only these devices or to move all of these devices to another group.

Kaspersky Security Center Linux provides a broad range of *predefined selections* (for example, **Devices with Critical status, Protection is disabled, Active threats are detected**). Predefined selections cannot be deleted. You can also create and configure additional *user-defined selections*.

In user-defined selections, you can set the search scope and select all devices, managed devices, or unassigned devices. Search parameters are specified in the conditions. In the device selection you can create several conditions with different search parameters. For example, you can create two conditions and specify different IP ranges in each of them. If several conditions are specified, a selection displays the devices that meet any of the conditions. By contrast, search parameters within a condition are superimposed. If both an IP range and the name of an installed application are specified in a condition, only those devices will be displayed where both the application is installed and the IP address belongs to the specified range.

## Viewing the device list from a device selection

Kaspersky Security Center Linux allows you to view the list of devices from a device selection.



*To view the device list from the device selection:*

1. In the main menu, go to the **Assets (Devices)** → **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 **Assets (Devices) → 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 **OK** 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 **Assets (Devices) → 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](#) ?

If this option is enabled, the specified selection condition will be inverted. The selection will include all devices that do not meet the condition.

By default, this option is disabled.

## Network infrastructure

In the **Network** subsection, you can specify the criteria that will be used to include devices in the selection according to their network data:

- [Device name](#) ?

Windows network name (NetBIOS name) of the device, or the IPv4 or IPv6 address.

- [Domain](#) ?

Displays all devices included in the specified workgroup.

- [Administration group](#) ?

Displays devices included in the specified administration group.

- [Description](#) ?

Text in the device properties window: in the **Description** field of the **General** section.

To describe text in the **Description** field, you can use the following characters:

- Within a word:
  - \*. Replaces any string with any number of characters.

**Example:**

To describe words such as **Server** or **Server's**, you can enter **Server\***.

- ?. Replaces any single character.

**Example:**

To describe phrases such as **SUSE Linux Enterprise Server 12** or **SUSE Linux Enterprise Server 15**, you can enter **SUSE Linux Enterprise Server 1?**.

Asterisk (\*) or question mark (?) cannot be used as the first character in the query.

- To find several words:
  - Space. Displays all the devices whose descriptions contain any of the listed words.

**Example:**

To find a phrase that contains **Secondary** or **Virtual** words, you can include **Secondary Virtual** line in your query.

- +. When a plus sign precedes a word, all search results will contain this word.

**Example:**

To find a phrase that contains both **Secondary** and **Virtual**, enter the **+Secondary+Virtual** query.

- -. When a minus sign precedes a word, no search results will contain this word.

**Example:**

To find a phrase that contains **Secondary** and does not contain **Virtual**, enter the **+Secondary-Virtual** query.

- "<some text>". Text enclosed in quotation marks must be present in the text.

**Example:**

To find a phrase that contains **Secondary Server** word combination, you can enter **"Secondary Server"** in the query.

- [IP range](#) 

If this option is enabled, you can enter the initial and final IP addresses of the IP range in which the relevant devices must be included.

By default, this option is disabled.

- [Managed by a different Administration Server](#) 



Select one of the following values:

- **Yes.** A device moving rule only applies to client devices managed by other Administration Servers. These Servers are different from the Server on which you configure the device moving rule.
- **No.** The device moving rule only applies to client devices managed by the current Administration Server.
- **No value is selected.** The condition does not apply.

In the **Domain controller** subsection, you can configure criteria for including devices into a selection based on domain membership:

- [Device is in a domain organizational unit](#) 

If this option is enabled, the selection includes devices from the domain organizational unit specified in the entry field.

By default, this option is disabled.

- [This device is a member of the domain security group](#) 

If this option is enabled, the selection includes devices from the domain security group specified in the entry field.

By default, this option is disabled.

In the **Network activity** subsection, you can specify the criteria that will be used to include devices in the selection according to their network activity:

- [Acts as a distribution point](#) 

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The selection includes devices that act as distribution points.
- **No.** Devices that act as distribution points are not included in the selection.
- **No value is selected.** The criterion will not be applied.

- [Do not disconnect from the Administration Server](#) 

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Enabled.** The selection will include devices on which the **Do not disconnect from the Administration Server** check box is selected.
- **Disabled.** The selection will include devices on which the **Do not disconnect from the Administration Server** check box is cleared.
- **No value is selected.** The criterion will not be applied.

- [Connection profile switched](#) ⓘ

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The selection will include devices that connected to the Administration Server after the connection profile was switched.
- **No.** The selection will not include devices that connected to the Administration Server after the connection profile was switched.
- **No value is selected.** The criterion will not be applied.

- [Last connected to Administration Server](#) ⓘ

You can use this check box to set a search criterion for devices according to the time they last connected to the Administration Server.

If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last connection was established between Network Agent installed on the client device and the Administration Server. The selection will include devices that fall within the specified interval.

If this check box is cleared, the criterion will not be applied.

By default, this check box is cleared.

- [New devices detected by network poll](#) ⓘ

Searches for new devices that have been detected by network polling over the last few days.

If this option is enabled, the selection only includes new devices that have been detected by device discovery over the number of days specified in the **Detection period (days)** field.

If this option is disabled, the selection includes all devices that have been detected by device discovery.

By default, this option is disabled.

- [Device is visible](#) ⓘ

In the drop-down list, you can set up the criterion for including devices in the selection when performing search:

- **Yes.** The application includes in the selection devices that are currently visible in the network.
- **No.** The application includes in the selection devices that are currently invisible in the network.
- **No value is selected.** The criterion will not be applied.

## Device statuses

In the **Managed device status** subsection, you can configure criteria for including devices into a selection based on the description of the devices status from a managed application:

- [Device status](#) ⓘ

Drop-down list in which you can select one of the device statuses: *OK*, *Critical*, or *Warning*.

- [Real-time protection status](#) 

Drop-down list, in which you can select the real-time protection status. Devices with the specified real-time protection status are included in the selection.

- [Device status description](#) 

In this field, you can select the check boxes next to conditions that, if met, assign one of the following statuses to the device: *OK*, *Critical*, or *Warning*.

In the **Status of components in managed applications** subsection, you can configure criteria for including devices in a selection according to the statuses of components in managed applications:

- [Data Leakage Prevention status](#) 

Search for devices by the status of Data Leakage Prevention (*No data from device*, *Stopped*, *Starting*, *Paused*, *Running*, *Failed*).

- [Collaboration servers protection status](#) 

Search for devices by the status of server collaboration protection (*No data from device*, *Stopped*, *Starting*, *Paused*, *Running*, *Failed*).

- [Anti-virus protection status of mail servers](#) 

Search for devices by the status of Mail Server protection (*No data from device*, *Stopped*, *Starting*, *Paused*, *Running*, *Failed*).

- [Endpoint Sensor status](#) 

Search for devices by the status of the Endpoint Sensor component (*No data from device*, *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 **Operating system** 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.

- [Operating system 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.

- [Operating system bit size](#) ?

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.

- [Operating system 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 build number. You can also configure searching for all build numbers except the specified one.

- [Operating system release number](#) ?

This setting is applicable to Windows operating systems only.

The release identifier (ID) of the operating system. You can specify whether the selected operating system must have an equal, earlier, or later release ID. You can also configure searching for all release ID numbers except the specified one.

In the **Virtual machines** section, you can set up the criteria to include devices in the selection according to whether these are virtual machines or part of virtual desktop infrastructure (VDI):

- [This is a virtual machine](#) ?

In the drop-down list, you can select the following options:

- **Undefined.**
- **No.** Find devices that are not virtual machines.
- **Yes.** Find devices that are virtual machines.

- [Virtual machine type](#) ?

In the drop-down list, you can select the virtual machine manufacturer.

This drop-down list is available if the **Yes** or **Not important** value is selected in the **This is a virtual machine** drop-down list.

- [Part of Virtual Desktop Infrastructure](#) 

In the drop-down list, you can select the following options:

- **Undefined.**
- **No.** Find devices that are not part of Virtual Desktop Infrastructure.
- **Yes.** Find devices that are part of the Virtual Desktop Infrastructure (VDI).

In the **Hardware registry** subsection, you can configure criteria for including devices into a selection based on their installed hardware:

Ensure that the lshw utility is installed on Linux devices from which you want to fetch hardware details. Hardware details fetched from virtual machines may be incomplete depending on the hypervisor used.

- [Device](#) 

In the drop-down list, you can select a unit type. All devices with this unit are included in the search results. The field supports the full-text search.

- [Vendor](#) 

In the drop-down list, you can select the name of a unit manufacturer. All devices with this unit are included in the search results. The field supports the full-text search.

- [Device name](#) 

The device with the specified name is included in the selection.

- [Description](#) 

Description of the device or hardware unit. Devices with the description specified in this field are included in the selection.

A device's description in any format can be entered in the properties window of that device. The field supports the full-text search.

- [Device vendor](#) 

Name of the device manufacturer. Devices produced by the manufacturer specified in this field are included in the selection.

You can enter the manufacturer's name in the properties window of a device.

- **[Serial number](#)** 

All hardware units with the serial number specified in this field will be included in the selection.

- **[Inventory number](#)** 

Equipment with the inventory number specified in this field will be included in the selection.

- **[User](#)** 

All hardware units of the user specified in this field will be included in the selection.

- **[Location](#)** 

Location of the device or hardware unit (for example, at the HQ or a branch office). Computers or other devices that are deployed at the location specified in this field will be included in the selection.

You can describe the location of a device in any format in the properties window of that device.

- **[CPU clock rate, in MHz, from](#)** 

The minimum clock rate of a CPU. Devices with a CPU that matches the clock rate range specified in the entry fields (inclusive) will be included in the selection.

- **[CPU clock rate, in MHz, to](#)** 

The maximum clock rate of a CPU. Devices with a CPU that matches the clock rate range specified in the entry fields (inclusive) will be included in the selection.

- **[Number of virtual CPU cores, from](#)** 

The minimum number of virtual CPU cores. Devices with a CPU that matches the range of the virtual cores number specified in the entry fields (inclusive) will be included in the selection.

- **[Number of virtual CPU cores, to](#)** 

The maximum number of virtual CPU cores. Devices with a CPU that matches the range of the virtual cores number specified in the entry fields (inclusive) will be included in the selection.

- **[Hard drive volume, in GB, from](#)** 

The minimum volume of the hard drive on the device. Devices with a hard drive that matches the volume range specified in the entry fields (inclusive) will be included in the selection.

- **[Hard drive volume, in GB, to](#)** 

The maximum volume of the hard drive on the device. Devices with a hard drive that matches the volume range specified in the entry fields (inclusive) will be included in the selection.

- [RAM size, in MB, from](#) ?

The minimum size of the device RAM. Devices with RAM that matches the size range specified in the entry fields (inclusive) will be included in the selection.

- [RAM size, in MB, to](#) ?

The maximum size of the device RAM. Devices with RAM that matches the size range specified in the entry fields (inclusive) will be included in the selection.

## Third-party software details

In the **Applications registry** subsection, you can set up the criteria to search for devices according to applications installed on them:

- [Application name](#) ?

Drop-down list in which you can select an application. Devices on which the specified application is installed, are included in the selection.

- [Application version](#) ?

Entry field in which you can specify the version of selected application.

- [Vendor](#) ?

Drop-down list in which you can select the manufacturer of an application installed on the device.

- [Application status](#) ?

A drop-down list in which you can select the status of an application (*Installed, Not installed*). Devices on which the specified application is installed or not installed, depending on the selected status, will be included in the selection.

- [Find by update](#) ?

If this option is enabled, search will be performed using the details of updates for applications installed on the relevant devices. After you select the check box, the **Application name**, **Application version**, and **Application status** fields change to **Update name**, **Update version**, and **Status** respectively.

By default, this option is disabled.

- [Name of incompatible security application](#) ?

Drop-down list in which you can select third-party security applications. During the search, devices on which the specified application is installed, are included in the selection.

- [Application tag](#) ?

In the drop-down list, you can select the application tag. All devices that have installed applications with the selected tag in the description are included in the device selection.

- [Apply to devices without the specified tags](#) 

If this option is enabled, the selection includes devices with descriptions that contain none of the selected tags.

If this option is disabled, the criterion is not applied.

By default, this option is disabled.

In the **Vulnerabilities and updates** subsection, you can specify the criteria that will be used to include devices in the selection according to their Windows Update source:

- [WUA is switched to Administration Server](#) 

You can select one of the following search options from the drop-down list:

- **Yes.** If this option is selected, the search results will include devices that receive updates through Windows Update from the Administration Server.
- **No.** If this option is selected, the results will include devices that receive updates through Windows Update from another sources.

## Details of Kaspersky applications

In the **Kaspersky applications** subsection, you can configure criteria for including devices in a selection based on the selected managed application:

- [Application name](#) 

In the drop-down list, you can set a criterion for including devices in a selection when search is performed by the name of a Kaspersky application.

The list provides only the names of applications with management plug-ins installed on the administrator's workstation.

If no application is selected, the criterion will not be applied.

- [Application version](#) 

In the entry field, you can set a criterion for including devices in a selection when search is performed by the version number of a Kaspersky application.

If no version number is specified, the criterion will not be applied.

- [Critical update name](#) 

In the entry field, you can set a criterion for including devices in a selection when search is performed by application name or by update package number.

If the field is left blank, the criterion will not be applied.



- [Application status](#) 

A drop-down list in which you can select the status of an application (*Installed, Not installed*). Devices on which the specified application is installed or not installed, depending on the selected status, will be included in the selection.

- [Select the period of the last update of modules](#) 

You can use this option to set a criterion for searching devices by time of the last update of modules of applications installed on those devices.

If this check box is selected, in the entry fields you can specify the time interval (date and time) during which the last update of modules of applications installed on those devices was performed.

If this check box is cleared, the criterion will not be applied.

By default, this check box is cleared.

- [Device is managed through Administration Server](#) 

In the drop-down list, you can include in the selection the devices managed through Kaspersky Security Center Linux:

- **Yes.** The application includes in the selection devices managed through Kaspersky Security Center Linux.
- **No.** The application includes devices in the selection if they are not managed through Kaspersky Security Center Linux.
- **No value is selected.** The criterion will not be applied.

- [Security application is installed](#) 

In the drop-down list, you can include in the selection all devices with the security application installed:

- **Yes.** The application includes in the selection all devices with the security application installed.
- **No.** The application includes in the selection all devices with no security application installed.
- **No value is selected.** The criterion will not be applied.

In the **Anti-virus protection** subsection, you can set up the criteria for including devices in a selection based on their protection status:

- [Databases released](#) 

If this option is selected, you can search for client devices by anti-virus database release date. In the entry fields you can set the time interval, on the basis of which the search is performed.

By default, this option is disabled.

- [Database records count](#) 

If this option is enabled, you can search for client devices by number of database records. In the entry fields you can set the lower and upper threshold values for anti-virus database records.

By default, this option is disabled.

- [Last scanned](#) ⓘ

If this check option is enabled, you can search for client devices by time of the last malware scan. In the entry fields you can specify the time period within which the last malware scan was performed.

By default, this option is disabled.

- [Threats detected](#) ⓘ

If this option is enabled, you can search for client devices by number of viruses detected. In the entry fields you can set the lower and upper threshold values for the number of viruses found.

By default, this option is disabled.

In the **Encryption** subsection, you can configure the criterion for including devices in a selection based on the selected encryption algorithm:

#### [Encryption algorithm](#) ⓘ

Advanced Encryption Standard (AES) symmetrical block cipher algorithm. In the drop-down list, you can select the encryption key size (56-bit, 128-bit, 192-bit, or 256-bit).

Available values: *AES56*, *AES128*, *AES192*, and *AES256*.

The **Application components** subsection contains the list of components of those applications that have corresponding management plug-ins installed in Kaspersky Security Center Web Console.

In the **Application components** subsection, you can specify criteria for including devices in a selection according to the statuses and version numbers of the components that refer to the application that you select:

- [Status](#) ⓘ

Search for devices according to the component status sent by an application to the Administration Server. You can select one of the following statuses: *N/A*, *Stopped*, *Paused*, *Starting*, *Running*, *Failed*, *Not installed*, *Not supported by license*. If the selected component of the application installed on a managed device has the specified status, the device is included in the device selection.

Statuses sent by applications:

- *Stopped*—The component is disabled and not working at the moment.
- *Paused*—The component is suspended, for example, after the user has paused protection in the managed application.
- *Starting*—The component is currently in the process of initialization.
- *Running*—The component is enabled and working properly.
- *Failed*—An error has occurred during the component operation.
- *Not installed*—The user did not select the component for installation when configuring custom installation of the application.
- *Not supported by license*—The license does not cover the selected component.

Unlike other statuses, the *N/A* status is not sent by applications. This option shows that the applications have no information about the selected component status. For example, this can happen when the selected component does not belong to any of the applications installed on the device, or when the device is turned off.

- [Version](#) 

Search for devices according to the version number of the component that you select in the list. You can type a version number, for example `3.4.1.0`, and then specify whether the selected component must have an equal, earlier, or later version. You can also configure searching for all versions except the specified one.

## Tags

In the **Tags** section, you can configure criteria for including devices into a selection based on key words (tags) that were previously added to the descriptions of managed devices:

### [Apply if at least one specified tag matches](#)

If this option is enabled, the search results will show devices with descriptions that contain at least one of the selected tags.

If this option is disabled, the search results will only show devices with descriptions that contain all the selected tags.

By default, this option is disabled.

To add tags to the criterion, click the **Add** button, and select tags by clicking the **Tag** entry field. Specify whether to include or exclude the devices with the selected tags in the device selection.

- [Must be included](#) 

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.

- [Must be excluded](#) 

If this option is selected, the search results will display the devices whose descriptions do not contain the selected tag. To find devices, you can use the asterisk, which stands for any string with any number of characters.

## Users

In the **Users** section, you can set up the criteria to include devices in the selection according to the accounts of users who have logged in to the operating system.

- [Last user who logged in to the system](#) 

If this option is enabled, you can select the user account for configuring the criterion. The search results include devices on which the selected user performed the last login to the system.

- [User who logged in to the system at least once](#) 

If this option is enabled, click the **Browse** button to specify a user account. The search results include devices on which the specified user logged in to the system at least once.

## Exporting the device list from a device selection

Kaspersky Security Center Linux allows you to save information about devices from a device selection and export it as a CSV or a TXT file.

*To export the device list from the device selection:*

1. [Open the table with the devices](#) from the device selection.
2. Use one of the following ways to select the devices that you want to export:
  - To select particular devices, select the check boxes next to them.
  - To select all devices from the current table page, select the check box in the device table header, and then select the **Select all on current page** check box.
  - To select all devices from the table, select the check box in the device table header, and then select the **Select all** check box.
3. Click the **Export to CSV** or **Export to TXT** button. All information about the selected devices included in the table will be exported.

Note that if you applied a filter criterion to the device table, only the filtered data from the displayed columns will be exported.

## Removing devices from administration groups in a selection

When working with a device selection, you can remove devices from administration groups right in this selection, without switching to the administration groups from which these devices must be removed.

*To remove devices from administration groups:*

1. In the main menu, go to **Assets (Devices) → Device selections** or **Discovery & deployment → Device selections**.

2. In the selection list, click the name of the device selection.

The page displays a table with information about the devices included in the device selection.

3. Select the devices that you want to remove, and then click **Delete**.

The selected devices are removed from their respective administration groups.

## Device tags

This section describes device tags, and provides instructions for creating and modifying them as well as for tagging devices manually or automatically.

## About device tags

Kaspersky Security Center Linux allows 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 Security Center Linux 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, you can set up a rule that will assign the [CentOS] tag to all devices running CentOS operating system. Then, you can use this tag when creating a device selection; this will help you sort all CentOS devices and assign them a task.

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 **Assets (Devices) → 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 the 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 **Assets (Devices) → 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 the 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 **Assets (Devices) → Tags → Device tags**.
2. In the list, select the device tag that you want to delete.
3. 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 remove the tag from your device, 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 **Assets (Devices) → Tags → Device tags**.
2. Click the **View devices** link next to the tag for which you want to view assigned devices.

The list of devices that appears shows only those devices to which the tag is assigned.

To return to the list of device tags, click the **Back** button of your browser.

## Viewing tags assigned to a device

*To view tags assigned to a device:*

1. In the main menu, go to **Assets (Devices) → Managed devices**.
2. Click the name of the device whose tags you want to view.
3. In the device properties window that opens, select the **Tags** tab.

The list of tags assigned to the selected device is displayed.

You can [assign another tag](#) to the device or [remove an already assigned tag](#). You can also see all device tags that exist on the Administration Server.

## Tagging a device manually

*To assign a tag to a device manually:*

1. [View tags assigned to the device to which you want to assign another tag](#).

2. Click **Add**.

3. In the window that opens, do one of the following:

- To create and assign a new tag, select **Create new tag**, and then specify the name of the new tag.
- To select an existing tag, select **Assign existing tag**, and then select the necessary tag in the drop-down list.

4. Click **OK** to apply the changes.

5. Click **Save** to save the changes.

The selected tag is assigned to the device.

## Removing an assigned tag from a device

*To remove a tag from a device:*

1. In the main menu, go to **Assets (Devices) → Managed devices**.
2. Click the name of the device whose tags you want to view.
3. In the device properties window that opens, select the **Tags** tab.
4. Select the check box next to the tag that you want to remove.
5. At the top of the list, click the **Unassign tag** button.
6. In the window that opens, click **Yes**.

The tag is removed from the device.

The unassigned device tag is not deleted. If you want, you can [delete it manually](#).

You cannot manually remove tags assigned to the device by applications or Network Agent. To remove these tags, use the `klscflag` utility.

## Viewing rules for tagging devices automatically

*To view rules for tagging devices automatically,*

Do any of the following:

- In the main menu, go to **Assets (Devices) → Tags → Auto-tagging rules**.



- In the main menu, go to **Assets (Devices)** → **Tags** → **Device tags**, and then click the **Set up auto-tagging rules** link.
- [View tags assigned to a device](#) and then click the **Settings** 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 be more than 256 characters long.
  - b. Do any 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 any 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 the 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 **Add**.

A new rule settings window opens.

3. Configure the general properties of the rule:

a. In the **Rule name** field, enter the rule name.

The name cannot be more than 256 characters long.

b. Do one of the following:

- Enable the rule by switching the toggle button to **Rule enabled**.
- Disable the rule by switching the toggle button to **Rule disabled**.

c. In the **Tag** field, enter the new device tag name or select one of the existing device tags from the list.

The name cannot be more than 256 characters long.

4. In the conditions section, click the **Add** button to add a new condition.

A new condition settings window open.

5. Enter the condition name.

The name cannot be more than 256 characters long. The name must be unique within a rule.

6. Set up the triggering of the rule according to the following conditions. You can select multiple conditions.

- **Network**—Network properties of the device, such as DNS name of the device or device inclusion in an IP subnet.

If case sensitive collation is set for the database that you use for Kaspersky Security Center Linux, keep case when you specify a device DNS name. Otherwise, the auto-tagging rule will not work.

- **Applications**—Presence of Network Agent on the device, operating system type, version, and architecture.
- **Virtual machines**—Device belongs to a specific type of virtual machine.
- **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 the 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 **Delete**.
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](#).

## Data encryption and protection

Data encryption reduces the risk of unintentional leakage of sensitive and corporate data if your laptop or hard drive is stolen or lost. Also, data encryption allows you to prevent access by unauthorized users and applications.

You can use the data encryption feature if your network includes Windows-based managed devices with Kaspersky Endpoint Security for Windows installed. In this case, you can manage the following types of encryption:

- BitLocker Drive Encryption on devices running a Windows operating system for servers
- Kaspersky Disk Encryption on devices running a Windows operating system for 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](#).

To configure encryption, define the Kaspersky Endpoint Security for Windows policy in Kaspersky Security Center Linux. Kaspersky Endpoint Security for Windows performs encryption and decryption according to the active policy. For detailed instructions on how to configure rules and for a description of encryption features, see the [Kaspersky Endpoint Security for Windows Help](#).

Encryption management for a hierarchy of Administration Servers is currently not available in the Web Console. Use the primary Administration Server to manage encrypted devices.

You can show or hide some of the interface elements related to the encryption management feature by using the [user interface settings](#).

## Viewing the list of encrypted drives

In Kaspersky Security Center Linux, you can view details about encrypted drives and devices that are encrypted at the drive level. After the information on a drive is decrypted, the drive is automatically removed from the list.

*To view the list of encrypted drives,*

In the main menu, go to **Operations** → **Data encryption and protection** → **Encrypted drives**.

If the section is not on the menu, this means that it is hidden. In the [user interface settings](#), enable the **Show data encryption and protection** option to display the section.

You can export the list of encrypted drives to a CSV or TXT file. To do this, click the **Export to CSV** or **Export to TXT** button.

## Viewing the list of encryption events

When running data encryption or decryption tasks on devices, Kaspersky Endpoint Security for Windows sends Kaspersky Security Center Linux information about events of the following types:

- Cannot encrypt or decrypt a file, or create an encrypted archive, due to a lack of free disk space.
- Cannot encrypt or decrypt a file, or create an encrypted archive, due to license issues.
- Cannot encrypt or decrypt a file, or create an encrypted archive, due to missing access rights.
- The application has been prohibited from accessing an encrypted file.

- Unknown errors.

*To view a list of events that occurred during data encryption on devices,*

In the main menu, go to **Operations** → **Data encryption and protection** → **Encryption events**.

If the section is not on the menu, this means that it is hidden. In the [user interface settings](#), enable the **Show data encryption and protection** option to display the section.

You can export the list of encrypted drives to a CSV or TXT file. To do this, click the **Export to CSV** or **Export to TXT** button.

Alternatively, you can examine the list of encryption events for every managed device.

*To view the encryption events for a managed device:*

1. In the main menu, go to **Assets (Devices)** → **Managed devices**.
2. Click on the name of a managed device.
3. On the **General** tab, go to the **Protection** section.
4. Click the **View data encryption errors** link.

## Creating and viewing encryption reports

You can generate the following reports:

- Report on encryption status of managed devices. This report provides details about the data encryption of various managed devices. For example, the report shows the number of devices to which the policy with configured encryption rules applies. Also, you can find out, for instance, how many devices need to be rebooted. The report also contains information about the encryption technology and algorithm for every device.
- Report on encryption status of mass storage devices. This report contains similar information as the report on the encryption status of managed devices, but it provides data only for mass storage devices and removable drives.
- Report on rights to access encrypted drives. This report shows which user accounts have access to encrypted drives.
- Report on file encryption errors. This report contains information about errors that occurred when the data encryption or decryption tasks were run on devices.
- Report on blockage of access to encrypted files. This report contains information about blocking application access to encrypted files. This report is helpful if an unauthorized user or application tries to access encrypted files or drives.

You can [generate any report](#) in the **Monitoring & reporting** → **Reports** section. Alternatively, in the **Operations** → **Data encryption and protection** section, you can generate the following encryption reports:

- Report on encryption status of mass storage devices
- Report on rights to access encrypted drives

- Report on file encryption errors

To generate an encryption report in the **Data encryption and protection** section:

1. Make sure that you enabled the **Show data encryption and protection** option in the [Interface options](#).
2. In the main menu, go to **Operations** → **Data encryption and protection**.
3. Open one of the following sections:
  - **Encrypted drives** generates the report on encryption status of mass storage devices or the report on rights to access encrypted drives.
  - **Encryption events** generates the report on file encryption errors.
4. Click the name of the report that you want to generate.

The report generation starts.

## Granting access to an encrypted drive in offline mode

A user can request access to an encrypted device, for example, when Kaspersky Endpoint Security 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 Kaspersky Endpoint Security for Windows plug-in.
6. Follow the instructions provided in the [Kaspersky Endpoint Security for Windows Help](#) (see the instructions for Kaspersky Security Center Web Console at the end of the section).

After that, the user applies the received file to access the encrypted drive and read data stored on the drive.

## Changing the Administration Server for client devices

You can change the Administration Server to a different one for specific client devices. For this purpose, use the *Change Administration Server* task.

To change the Administration Server that manages client devices to a different Server:

1. Connect to the Administration Server that manages the devices.
2. [Create](#) the Administration Server change task.

The New task wizard starts. Follow the instructions of the wizard. In the **New task** window of the New task wizard, select the **Kaspersky Security Center 15** application and the **Change Administration Server** task type. After that, specify the devices for which you want to change the Administration Server:

- [Assign task to an administration group](#) 

The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

- [Specify device addresses manually or import addresses from a list](#) 

You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.


- [Assign task to a device selection](#) 

The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.

3. Run the created task.

After the task is complete, the client devices for which it was created are put under the management of the Administration Server specified in the task settings.

If the Administration Server supports encryption and data protection and you are creating a *Change Administration Server* task, a warning is displayed. The warning states that if any encrypted data is stored on devices, after the new Server begins managing the devices, users will be able to access only the encrypted data with which they previously worked. In other cases, no access to encrypted data is provided. For detailed descriptions of scenarios in which access to encrypted data is not provided, refer to the [Kaspersky Endpoint Security for Windows Help](#) .

## 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 **Assets (Devices) → 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, this 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, this 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, this option is enabled.

6. Click **Save**.

Your changes are saved and applied.

## Sending messages to device users

To send a message to users of devices:



1. In the main menu, go to **Assets (Devices)** → **Tasks**.
2. Click **Add**.  
The New task wizard starts.
3. In the **Task type** drop-down list, select **Send message to user**.
4. Select an option to specify the administration group, the device selection, or the devices to which the task applies.
5. Run the created task.

After the task is complete, the created message will be sent to the users of the selected devices. The **Send message to user** task is available only for devices running Windows.

## Turning on, turning off, and restarting client devices remotely

Kaspersky Security Center Linux allows you to manage client devices remotely by turning on, shutting down, or restarting them.

*To remotely manage client devices:*

1. In the main menu, go to **Assets (Devices)** → **Tasks**.
2. Click **Add**.  
The New task wizard starts.
3. In the **Task type** drop-down list, select **Manage devices**.
4. Select an option to specify the administration group, the device selection, or the devices to which the task applies.
5. Select the command (turn on, turn off, or restart). Optionally, specify the user prompt message and the **Wait time before forced closure of applications in blocked sessions (min)** option for the turn off and restart commands.
6. Run the created task.

After the task is complete, the command (turn on, turn off, or restart) will be executed on the selected devices.

# Deploying Kaspersky applications

This section describes Kaspersky applications deployment on client devices in your organization by means of Kaspersky Security Center Web Console.

## Scenario: Kaspersky applications deployment

This scenario explains how to deploy Kaspersky applications through Kaspersky Security Center Web Console. You can use the [quick start wizard](#) and [Protection deployment wizard](#), or you can complete all necessary steps manually.

The following applications are available for deployment by using Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

## Stages

Kaspersky applications deployment proceeds in stages:

### 1 Downloading management web plug-in for the application

This stage is handled by the quick start wizard. If you choose not to run the wizard, download the plug-ins manually.

### 2 Downloading and creating installation packages

This stage is handled by the quick start wizard.

The quick start wizard allows you to download the installation package with the management web plug-in. If you did not select this option when running the wizard, or if you did not run the wizard at all, you must [download the package manually](#).

If you cannot install Kaspersky applications by means of Kaspersky Security Center Linux on some devices, for example, on remote employees' devices, you can [create stand-alone installation packages](#) for applications. If you use stand-alone packages to install Kaspersky applications, you do not have to create and run a remote installation task, nor create and configure tasks for Kaspersky Endpoint Security for Windows.

Alternatively, you can [download the distribution packages for Network Agent and security applications from the Kaspersky website](#) <sup>2</sup>. If the remote installation of the applications is not possible for some reason, you can use the downloaded distribution packages to install the applications locally.

### 3 Creating, configuring, and running the remote installation task

This step is part of the Protection deployment wizard. If you choose not to run the Protection deployment wizard, [you must create this task manually](#), and configure it manually.

You also can manually create several remote installation tasks for different administration groups or different device selections. You can deploy different versions of one application in these tasks.

Make sure that all the devices on your network are discovered; then run the remote installation task (or tasks).

If you want to install Network Agent on devices with the SUSE Linux Enterprise Server 15 operating system, [install the insserv-compat package](#) first to configure Network Agent.

#### 4 Creating and configuring tasks

The *Update* task of Kaspersky Endpoint Security must be configured.

This step is part of the quick start wizard: the task is created and configured automatically with the default settings. If you did not run the wizard, [you must create this task manually](#) and configure it manually. If you use the quick start wizard, make sure that the [schedule for the task](#) meets your requirements. (By default, the scheduled start for the task is set to **Manually**, but you might want to choose another option.)

#### 5 Creating policies

Create the policy for Kaspersky Endpoint Security [manually](#), or through the quick start wizard. You can use the default settings of the policy; you can also [modify the default settings](#) of the policy according to your needs at any time.

#### 6 Verifying the results

Make sure that deployment was completed successfully: you have policies and tasks for each application, and these applications are installed on the managed devices.

## Results

Completion of the scenario yields the following:

- All required policies and tasks for the selected applications are created.
- The schedules of tasks are configured according to your needs.
- The selected applications are deployed, or scheduled to be deployed, on the selected client devices.

## Adding management plug-ins for Kaspersky applications

To deploy a Kaspersky application, such as Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Windows, you must add and install the management web plug-in for the application.

*To download a management web plug-in for a Kaspersky application:*

1. In the main menu, go to **Settings** → **Web plug-ins**.
2. In the window that opens, click the **Add** button.  
The list of available plug-ins is displayed.
3. In the list of available plug-ins, select the plug-in you want to download (for example, Kaspersky Endpoint Security for Linux) by clicking on its name.  
A plug-in description page is displayed.
4. On the plug-in description page, click **Install plug-in**.
5. When the installation is complete, click **OK**.

The management web plug-in is downloaded with the default configuration and displayed in the list of management web plug-ins.

You can add plug-ins and update downloaded plug-ins from a file. You can download management web plug-ins from the [Kaspersky website](#).

*To download or update management web plug-in from a file:*

1. In the main menu, go to **Settings** → **Web plug-ins**.
2. Specify the file of the plug-in and the signature of the file:
  - Click **Add from file** to download a plug-in from a file.
  - Click **Update from file** to download an update of a plug-in from a file.
3. Specify the file and signature of the file.
4. Download the specified files.

The management web plug-in is downloaded from the file and displayed in the list of management web plug-ins.

## Downloading and creating installation packages for Kaspersky applications

You can create installation packages for Kaspersky applications from Kaspersky web servers if your Administration Server has access to the internet.

*To download and create installation package for Kaspersky application:*

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 for Kaspersky applications in the list of [onscreen notifications](#). If there are notifications about a new package, you can click the link next to the notification and proceed to the list of available installation packages.

A list of installation packages available on Administration Server is displayed.

2. Click **Add**.

The New package wizard starts. Proceed through the wizard by using the **Next** button.

3. On the first page of the wizard, select **Create an installation package for a Kaspersky application**.

A list of available installation packages on Kaspersky web servers appears. The list contains installation packages only for those applications that are compatible with the current version of Kaspersky Security Center Linux.

4. Click the name of an installation package, for example, Kaspersky Endpoint Security for Linux.

A window opens with information about the installation package.

You can download and use an installation package which includes cryptographic tools that implement strong encryption, if it complies with applicable laws and regulations. To download the installation package of Kaspersky Endpoint Security for Windows valid for the needs of your organization, consult the legislation of the country where the client devices of your organization are located.

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

If a distribution package can not be converted to an installation package, the **Download distribution package** button instead of the **Download and create installation package** is displayed.

The downloading of the installation package to Administration Server starts. You can close the wizard's window or proceed to the next step of the instruction. If you close the wizard's window, the download process will continue in background mode.

If you want to track an installation package download process:

- a. In the main menu, go to **Operations** → **Repositories** → **Installation packages** → **In progress ()**.
- b. Track the operation progress in the **Download progress** column and the **Download status** column of the table.

When the process is complete, the installation package is added to the list on the **Downloaded** tab. If the download process stops and the download status switches to **Accept EULA**, then click the installation package name, and then proceed to the next step of the instruction.

If the size of data contained in the selected distribution package exceeds the current limit, an error message is displayed. You can [change the limit value](#) and then proceed with the installation package creation.

6. For some Kaspersky applications, 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 the End User License Agreement (EULA).
- b. Read the EULA that is displayed on the screen, and click **Accept**.

The downloading continues after you accept the EULA. If you click **Decline**, the download is stopped.

7. When the downloading is complete, click the **Close** button.

The selected installation package is downloaded to the Administration Server shared folder, to the Packages subfolder. After downloading, the installation package is displayed in the list of installation packages.

## Creating installation packages from a file

You can use custom installation packages to do the following:

- To install any application (such as a text editor) on a client device, for example, by means of a [task](#).
- To [create a stand-alone installation package](#).

A custom installation package is a folder with a set of files. The source to create a custom installation package is an *archive file*. The archive file contains a file or files that must be included in the custom installation package.

While creating a custom installation package, you can specify command-line parameters, for example, to install the application in silent mode.

*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 the Administration Server is displayed.

2. Click **Add**.

The New package wizard starts. Proceed through the wizard by using the **Next** button.

3. On the first page of the wizard, select **Create an installation package from a file**.

4. On the next page of the wizard, specify the package name and click the **Browse** button.

5. In the window that opens, choose an archive file located on the available disks.

You can upload a ZIP, CAB, TAR, or TAR.GZ archive file. It is not possible to create an installation package from an SFX (self-extracting archive) file.

File upload to the Administration Server starts.

6. If you specified a file of a Kaspersky application, you may be prompted to read and accept the [End User License Agreement](#) (EULA) for the application. To continue, you must accept the EULA. Select the **Accept the terms and conditions of this End User License Agreement** option only if you have fully read, understand and accept the terms of the EULA.

Additionally, you may be prompted to read and accept the [Privacy Policy](#). To continue, you must accept the Privacy Policy. Select the **I accept the Privacy Policy** option only if you understand and agree that your data will be handled and transmitted (including to third countries) as described in the Privacy Policy.

7. On the next page of the wizard, select a file (from the list of files that are extracted from the chosen archive file) and specify the command-line parameters of an executable file.

You can specify command-line parameters to install the application from the installation package in a silent mode. Specifying command-line parameters is optional.

The process to create the installation package is started.

The wizard informs you when the process is finished.

If the installation package is not created, an appropriate message is displayed.

8. Click the **Finish** button to close the wizard.

The installation package that you created is downloaded to the Packages subfolder of the [Administration Server shared folder](#). After downloading, the installation package appears in the list of installation packages.

In the list of installation packages available on Administration Server, by clicking the link with the name of a custom installation package, you can:

- View the following properties of an installation package:
  - **Name**. Custom installation package name.
  - **Source**. Application vendor name.

- **Application.** Application name packed into the custom installation package.
  - **Version.** Application version.
  - **Language.** Language of the application packed into the custom installation package.
  - **Size (MB).** Size of the installation package.
  - **Operating system.** Type of the operating system for which the installation package is intended.
  - **Created.** Installation package creation date.
  - **Modified.** Installation package modification date.
  - **Type.** Type of the installation package.
- Change the command-line parameters.

## Creating stand-alone installation packages

You and device users in your organization can use stand-alone installation packages to install applications on devices manually.

A stand-alone installation package is an executable file (Installer.exe) that you can store on the Web Server or in the shared folder, send by email, or transfer to a client device by another method. On the client device, the user can run the received file locally to install an application without involving Kaspersky Security Center Linux. You can create stand-alone installation packages for Kaspersky applications and for third-party applications. To create a stand-alone installation package for a third-party application you must [create a custom installation package](#).

Be sure that stand-alone installation package is not available for third persons.

*To create a stand-alone installation package:*

1. 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. In the list of installation packages, select an installation package and, above the list, click the **Deploy** button.
3. Select the **Using a stand-alone package** option.

The Stand-alone installation package creation wizard starts. Proceed through the wizard by using the **Next** button.

4. On the first page of the wizard, 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.

By default, this option is enabled. It is recommended to enable this option if you are not sure whether Network Agent is installed on the device. If Network Agent is already installed on the device, after the stand-alone installation package with Network Agent installed Network Agent will be updated to the newer version.

If you disable this option, Network Agent will not be installed on the device and the device will be unmanaged. If a stand-alone installation package for the selected application already exists on Administration Server, the wizard informs you about this fact. In this case, you must select one of the following actions:

- **Create stand-alone installation package.** Select this option, for example, if you want to create a stand-alone installation package for a new application version and also want to retain a stand-alone installation package that you created for a previous application version. The new stand-alone installation package is placed in another folder.
- **Use existing stand-alone installation package.** Select this option if you want to use an existing stand-alone installation package. The process of package creation will not be started.
- **Rebuild existing stand-alone installation package.** Select this option if you want to create a stand-alone installation package for the same application again. The stand-alone installation package is placed in the same folder.

5. On the **Move to list of managed devices** page of the wizard, by default the **Do not move devices** option is selected. 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.

6. On the next page of the wizard, when the process of the stand-alone installation package creation is finished, click the **FINISH** button.

The Stand-alone installation package creation wizard closes.

The stand-alone installation package is created and placed in the PkgInst subfolder of the [Administration Server shared folder](#). You can view the list of stand-alone packages by clicking the **View the list of stand-alone packages** button above the list of installation packages.

## Changing the limit on the size of custom installation package data

The total size of data unpacked during creation of a custom installation package is limited. The default limit is 1 GB.

If you attempt to upload an archive file that contains data exceeding the current limit, an error message is displayed. You might have to increase this limit value when creating installation packages from large distribution packages.

*To change the limit value for the custom installation package size:*

1. On the Administration Server device, run the command prompt under the account that was used to [install Administration Server](#).
2. Change your current directory to the Kaspersky Security Center Linux installation folder (usually, /opt/kaspersky/ksc64/sbin).
3. Depending on the type of Administration server installation, enter one of the following commands under the root account:

- Normal local installation:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes >
```



- Installation on the Kaspersky Security Center Linux failover cluster:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <number of bytes> --stp
klfoc
```

Where <number of bytes> is a number of bytes in hexadecimal or decimal format.

For example, if the required limit is 2 GB, you can specify the decimal value 2147483648 or the hexadecimal value 0x80000000. In this case, for a local installation of Administration Server, you can use the following command:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
```

The limit on the size of custom installation package data is changed.

## Installing Network Agent for Linux in silent mode (with an answer file)

You can install Network Agent on Linux devices by using an answer file—a text file that contains a custom set of installation parameters: variables and their respective values. Using this answer file allows you to run an installation in silent mode, that is, without user participation.

*To perform installation of Network Agent for Linux in silent mode:*

1. [Prepare the relevant Linux device for remote installation](#). Download and create the remote installation package, by using a .deb or .rpm package of Network Agent, by means of any suitable package management system.
2. 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.
3. Read the [End User License Agreement](#). Follow the steps below only if you understand and accept the terms of the End User License Agreement.
4. Set the value of the KLAUTOANSWERS environment variable by entering the full name of the answer file (including the path), for example, as follows:  

```
export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
```
5. Create the answer file (in TXT format) in the directory that you have specified in the environment variable. Add to the answer file a list of variables in the VARIABLE\_NAME=variable\_value format, each variable on a separate line.

For correct usage of the answer file, you must include in it a minimum set of the three required variables:

- KLNAGENT\_SERVER
- KLNAGENT\_AUTOINSTALL
- EULA\_ACCEPTED

You can also add any optional variables to use more specific parameters of your remote installation. The following table lists all of the variables that can be included in the answer file:

[Variables of the answer file used as parameters of Network Agent for Linux installation in silent mode](#) 

| Variable name           | Required | Description                                                                                                                                              | Possible values                                                                                                                                                                                                                           |
|-------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KLNAGENT_SERVER         | Yes      | Contains the Administration Server name presented as fully qualified domain name (FQDN) or IP address.                                                   | DNS name or IP address.                                                                                                                                                                                                                   |
| KLNAGENT_AUTOINSTALL    | Yes      | Defines whether silent installation mode is enabled.                                                                                                     | 1—Silent mode is enabled; the user is not prompted for any actions during installation.<br><br>Other—Silent mode is disabled; the user may be prompted for actions during installation.                                                   |
| EULA_ACCEPTED           | Yes      | Defines whether the user accepts the End User License Agreement (EULA) of Network Agent; when missing, can be interpreted as non-acceptance of the EULA. | 1—I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement.<br><br>Other or not specified—I do not accept the terms of the License Agreement (installation is not performed). |
| KLNAGENT_PROXY_USE      | No       | Defines whether connection with the Administration Server will use proxy settings. The default value is 0.                                               | 1—Proxy settings are used.<br><br>Other—Proxy settings are not used.                                                                                                                                                                      |
| KLNAGENT_PROXY_ADDR     | No       | Defines the address of the proxy server used for connection with the Administration Server.                                                              | DNS name or IP address.                                                                                                                                                                                                                   |
| KLNAGENT_PROXY_LOGIN    | No       | Defines the user name used for login to the proxy server.                                                                                                | Any existing user name.                                                                                                                                                                                                                   |
| KLNAGENT_PROXY_PASSWORD | No       | Defines the user password used for login to the proxy server.                                                                                            | Any set of alphanumeric characters allowed by the password format in the operating system.                                                                                                                                                |
| KLNAGENT_VM_VDI         | No       | Defines whether Network Agent is installed on an image                                                                                                   | 1—Network Agent is installed on an                                                                                                                                                                                                        |

|                      |    |                                                                             |                                                                                                                                                                                                                                                                                        |
|----------------------|----|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |    | for creation of dynamic virtual machines.                                   | image, which is subsequently used for creation of dynamic virtual machines.<br><br>Other—No image is used during installation.                                                                                                                                                         |
| KLNAGENT_VM_OPTIMIZE | No | Defines whether the Network Agent settings are optimal for hypervisor.      | 1—The default local settings of Network Agent are modified so that they allow optimized usage on hypervisor.                                                                                                                                                                           |
| KLNAGENT_TAGS        | No | Lists the tags assigned to the Network Agent instance.                      | One or multiple tag names separated with semicolon.                                                                                                                                                                                                                                    |
| KLNAGENT_UDP_PORT    | No | Defines the UDP port used by Network Agent. The default value is 15000.     | Any existing port number.                                                                                                                                                                                                                                                              |
| KLNAGENT_PORT        | No | Defines the non-TLS port used by Network Agent. The default value is 14000. | Any existing port number.                                                                                                                                                                                                                                                              |
| KLNAGENT_SSLPORT     | No | Defines the TLS port used by Network Agent. The default value is 13000.     | Any existing port number.                                                                                                                                                                                                                                                              |
| KLNAGENT_USESSL      | No | Defines whether Transport Layer Security (TLS) is used for connection.      | 1 (default)—TLS is used.<br><br>Other—TLS is not used.                                                                                                                                                                                                                                 |
| KLNAGENT_GW_MODE     | No | Defines whether connection gateway is used.                                 | 1 (default)—The current settings are not modified (at the first call, no connection gateway is specified).<br><br>2—No connection gateway is used.<br><br>3—Connection gateway is used.<br><br>4—The Network Agent instance is used as connection gateway in demilitarized zone (DMZ). |
| KLNAGENT_GW_ADDRESS  | No | Defines the address of the connection gateway. The                          | DNS name or IP address.                                                                                                                                                                                                                                                                |

|  |                                                    |  |
|--|----------------------------------------------------|--|
|  | value is applicable only if<br>KLNAGENT_GW_MODE=3. |  |
|--|----------------------------------------------------|--|

## 6. Install Network Agent:

- To install Network Agent from an RPM package to a 32-bit operating system, execute the following command:  
`# rpm -i klnagent-<build number>.i386.rpm`
- To install Network Agent from an RPM package to a 64-bit operating system, execute the following command:  
`# rpm -i klnagent64-<build number>.x86_64.rpm`
- To install Network Agent from an RPM package on a 64-bit operating system for the Arm architecture, execute the following command:  
`# rpm -i klnagent64-<build number>.aarch64.rpm`
- To install Network Agent from a DEB package to a 32-bit operating system, execute the following command:  
`# apt-get install ./klnagent_<build number>_i386.deb`
- To install Network Agent from a DEB package to a 64-bit operating system, execute the following command:  
`# apt-get install ./klnagent64_<build number>_amd64.deb`
- To install Network Agent from a DEB package on a 64-bit operating system for the Arm architecture, execute the following command:  
`# apt-get install ./klnagent64_<build number>_arm64.deb`

Installation of Network Agent for Linux starts in silent mode; the user is not prompted for any actions during the process.

## 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](#).

Before you begin:

- Make sure that the device on which you want to install Network Agent for Linux is running one of the [supported Linux distributions](#).
- Download the necessary Network Agent installation file from the [Kaspersky website](#).

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/ksc64/share/kaspersky\_astra\_pub\_key.gpg in the directory created in the previous step:

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

If the Kaspersky Security Center Linux distribution kit does not include the kaspersky\_astra\_pub\_key.gpg application key, you can download it by clicking the link:

[https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky\\_astra\\_pub\\_key.gpg](https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg).

5. Update the RAM disks:

```
update-initramfs -u -k all
```

Reboot the system.

6. Perform the [preparation steps common for any Linux device](#).

The device is prepared. You can now proceed to the [installation of Network Agent](#).

## Viewing the list of stand-alone installation packages

You can view the list of stand-alone installation packages and properties of each stand-alone installation package.

*To view the list of stand-alone installation packages for all installation packages:*

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

In the list of stand-alone installation packages, their properties are displayed as follows:

- **Package name.** Stand-alone installation package name that is automatically formed as the application name included in the package and the application version.
- **Application name.** Application name included in the stand-alone installation package.
- **Application version.**
- **Network Agent installation package name.** The property is displayed only if Network Agent is included in the stand-alone installation package.
- **Network Agent version.** The property is displayed only if Network Agent is included in the stand-alone installation package.
- **Size.** File size in MB.
- **Group.** Name of the group to which the client device is moved after Network Agent installation.
- **Created.** Date and time of the stand-alone installation package creation.

- **Modified.** Date and time of the stand-alone installation package modification.
- **Path.** Full path to the folder where the stand-alone installation package is located.
- **Web address.** Web address of the stand-alone installation package location.
- **File hash.** The property is used to certify that the stand-alone installation package was not changed by third-party persons and a user has the same file you have created and transferred to the user.

*To view the list of stand-alone installation packages for specific installation package:*

Select the installation package in the list and, above the list, click the **View the list of stand-alone packages** button.

In the list of stand-alone installation packages, you can do the following:

- Publish a stand-alone installation package on the Web Server by clicking the **Publish** button. Published stand-alone installation package is available for downloading for users whom you sent the link to the stand-alone installation package.
- Cancel publication of a stand-alone installation package on the Web Server by clicking the **Unpublish** button. Unpublished stand-alone installation package is available for downloading only for you and other administrators.
- Download a stand-alone installation package to your device by clicking the **Download** button.
- Send email with the link to a stand-alone installation package by clicking the **Send by email** button.
- Remove a stand-alone installation package by clicking the **Remove** button.

## Distributing installation packages to secondary Administration Servers

Kaspersky Security Center Linux allows you to [create installation packages](#) for Kaspersky applications and for third-party applications, as well as distribute installation packages to client devices and install applications from the packages. To optimize the load on the primary Administration Server, you can distribute installation packages to secondary Administration Servers. After that, the secondary Servers transmit the packages to client devices, and then you can perform the remote installation of the applications on your client devices.

*To distribute installation packages to secondary Administration Servers:*

1. Make sure that the secondary Administration Servers are connected to the primary Administration Server.
2. In the main menu, go to **Assets (Devices) → Tasks**.  
The list of tasks is displayed.
3. Click the **Add** button.  
The New task wizard starts. Follow the steps of the wizard.
4. On the **New task** page, from the **Application** drop-down list, select **Kaspersky Security Center**. Then, from the **Task type** drop-down list, select **Distribute installation package**, and then specify the task name.
5. On the **Task scope** page, select the devices to which the task is assigned in one of the following ways:

- If you want to create a task for all secondary Administration Servers in a specific administration group, select this group, and then create a group task for it.
  - If you want to create a task for specific secondary Administration Servers, select these Servers, and then create a task for them.
6. On the **Distributed installation packages** page, select the installation packages that are to be copied to the secondary Administration Servers.
  7. Specify an account to run the *Distribute installation package* task under this account. You can use your account and keep the **Default account** option enabled. Alternatively, you can specify that the task should be run under another account that has the necessary access rights. To do this, select the **Specify account** option, and then enter the credentials of that account.
  8. On the **Finish task creation** page, you can enable the **Open task details when creation is complete** option to open the task properties window, and then modify the default [task settings](#). Otherwise, you can configure the task settings later, at any time.
  9. Click the **Finish** button.

The task created for distributing installation packages to the secondary Administration Servers is displayed in the task list.
  10. You can run the task manually or wait for it to launch according to the schedule that you specified in the task settings.

After the task is complete, the selected installation packages are copied to the specified secondary Administration Servers.

## 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 following software is installed on the target Linux device:

- Sudo
- Perl language interpreter version 5.10 or later

2. Test the device configuration:

a. Check whether you can connect to the device through an SSH client (such as PuTTY).

If you cannot connect to the device, open the `/etc/ssh/sshd_config` file and make sure that the following settings have the respective values listed below:

PasswordAuthentication no

ChallengeResponseAuthentication yes

Do not modify the `/etc/ssh/sshd_config` file if you can connect to the device with no issues; otherwise, you may encounter SSH authentication failure when running a remote installation task.

Save the file (if necessary) and restart the SSH service by using the `sudo service ssh restart` command.

b. 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, find the line that starts with `%sudo` (or with `%wheel` if you are using the CentOS operating system). Under this line, specify the following: `<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.

3. 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
```

4. 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.

5. 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](#).

## 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. Download the Network Agent installation package [by using the application interface](#) or from the [Kaspersky website](#).
- c. To create a remote installation package, use the following files:
  - klnagent.kpd
  - ainstall.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`.

An error may be returned if you install Network Agent with SSH on devices running Fedora versions earlier than version 20. In this case, for successful installation of Network Agent, comment out the Defaults requiretty option (enclose it in comment syntax to remove it from parsed code) in the `/etc/sudoers` file. For a detailed description of the condition of the Defaults requiretty option that may cause problems during SSH connection, please refer to the [Bugzilla bugtracker website](#).

## Installing applications using a remote installation task

Kaspersky Security Center Linux allows you to install applications on devices remotely, using remote installation tasks. Those tasks are created and assigned to devices through a dedicated wizard. To assign a task to devices more quickly and easily, you can specify devices in the wizard window in one of the following ways:

- **Assign task to an administration group.** In this case, the task is assigned to devices included in an administration group created earlier.
- **Specify device addresses manually or import addresses from a list.** You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.
- **Assign task to a device selection.** In this case, the task is assigned to devices included in a selection created earlier. You can specify the default selection or a custom one that you created.

For correct remote installation on a device with no Network Agent installed, the following ports must be opened: a) TCP 139 and 445; b) UDP 137 and 138. By default, these ports are opened on all devices included in the domain. They are opened automatically by the [remote installation preparation utility](#).

## 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 **Assets (Devices)** → **Tasks**.
2. Click **Add**.  
The New task wizard starts.
3. In the **Task type** field, select **Install application remotely**.
4. 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.

- [Specify device addresses manually or import addresses from a list](#) ⓘ

You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

- [Assign task to a device selection](#) ⓘ

The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.

The *Install application remotely* task is created for the specified devices. If you selected the **Assign task to an administration group** option, the task is a group one.

5. At the **Task scope** step, specify an administration group, devices with specific addresses, or a device selection.  
The available settings depend on the option selected at the previous step.
6. At the **Installation packages** step, specify the following settings:
  - In the **Select installation package** field, select the installation package of an application that you want to install.

- In the **Force installation package download** settings group, specify how files that are required for the application installation are distributed to client devices:

- [Using Network Agent](#)

If this option is enabled, installation packages are delivered to client devices by Network Agent installed on those client devices.

If this option is disabled, installation packages are delivered using the operating system tools of client devices.

We recommend that you enable this option if the task has been assigned to devices with Network Agents installed.

By default, this option is enabled.

- [Using operating system resources through distribution points](#)

If this option is enabled, installation packages are transmitted to client devices using operating system tools through distribution points. You can select this option if there is at least one distribution point on the network.

If the **Using Network Agent** option is enabled, the files are delivered using operating system tools only if Network Agent tools are unavailable.

By default, this option is enabled for remote installation tasks that have been created on a virtual Administration Server.

The only way to install an application for Windows (including Network Agent for Windows) on a device that does not have Network Agent installed is by using a Windows-based distribution point. Therefore, when you install a Windows application:

- Select this option.
- Ensure that a distribution point is assigned for the target client devices.
- Ensure the distribution point is Windows-based.

- [Using operating system resources through Administration Server](#)

If this option is enabled, files are transmitted to client devices by using operating system tools of client devices through the Administration Server. You can enable this option if no Network Agent is installed on the client device, but the client device is in the same network as the Administration Server.

By default, this option is enabled.

- In the **Maximum number of concurrent downloads** field, specify the maximum allowed number of client devices to which Administration Server can simultaneously transmit the files.
- In the **Maximum number of installation attempts** field, specify the maximum allowed number of installer runs.

If the number of attempts specified in the parameter is exceeded, Kaspersky Security Center Linux does not start the installer on the device anymore. To restart the *Install application remotely* task, increase the value of the **Maximum number of installation attempts** parameter and start the task. Alternatively, you can create a new *Install application remotely* task.
- 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, this option is enabled.

- [Verify operating system type before downloading](#) 

Before transmitting the files to client devices, Kaspersky Security Center Linux checks if the Installation utility settings are applicable to the operating system of the client device. If the settings are not applicable, Kaspersky Security Center Linux does not transmit the files and does not attempt to install the application. For example, to install some application to devices of an administration group that includes devices running various operating systems, you can assign the installation task to the administration group, and then enable this option to skip devices that run an operating system other than the required one.

- [Prompt users to close running applications](#) 

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

- Select on which devices you want to install the application:

- [Install on all devices](#) 

The application will be installed even on devices managed by other Administration Servers.

This option is selected by default. You do not have to change this setting if you have only one Administration Server in your network.

- [Install only on devices managed through this Administration Server](#) 

The application will be installed only on devices managed by this Administration Server. Select this option if you have more than one Administration Server in your network and want to avoid conflicts between them.

- Specify whether devices must be moved to an administration group after installation:

- [Do not move devices](#) 

The devices remain in the groups in which they are currently located. The devices that have not been placed in any group remain unassigned.

- [Move unassigned devices to the selected group \(only a single group can be selected\)](#) 

The devices are moved to the administration group that you select.

Note that the **Do not move devices** option is selected by default. For security reasons, you might want to move the devices manually.

7. At the this step of the wizard, specify whether the devices must be restarted during installation of applications:

- [Do not restart the device](#) 

If this option is selected, the device will not be restarted after the security application installation.

- [Restart the device](#) 

If this option is selected, the device will be restarted after the security application installation.

8. If necessary, at the **Select accounts to access devices** step, add the accounts that will be used to start the *Install application remotely* task:

- [No account required \(Network Agent installed\)](#) 

If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running. If Network Agent has not been installed on client devices, this option is not available.

- [Account required \(Network Agent is not used\)](#) 

Select this option if Network Agent is not installed on the devices for which you assign the remote installation task. In this case, you can specify a user account to install the application.

To specify the user account under which the application installer will be run, click the **Add** button, select **Local 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.

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.

## 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 **Assets (Devices) → 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 settings:

- [Set a password for the root account \(only for deployment through SSH\)](#) 

If the `sudo` command cannot be used on the target device without specifying the password, select this option, and then specify the password for the root account. Kaspersky Security Center Linux transmits the password in an encrypted form to the target device, decrypts the password, and then starts the installation procedure on behalf of the root account with the specified password.

Kaspersky Security Center Linux does not use the account or the specified password to create an SSH connection.

- [Specify the path to a temporary folder with Execute permissions on the target device \(only for deployment through SSH\)](#)<sup>2</sup>

If the /tmp directory on the target device does not have the execute permission, select this option, and then specify the path to the directory with the execute permission. Kaspersky Security Center Linux uses the specified directory as a temporary directory to access via SSH. The application places the installation package in the directory and runs the installation procedure.

5. Click the **Save** button.

The specified task settings are saved.

## Replacing third-party security applications

Installation of Kaspersky security applications through Kaspersky Security Center Linux may require removal of third-party software that is incompatible with the application being installed. Kaspersky Security Center Linux provides several ways of removing the third-party applications.

### Removing incompatible applications when configuring remote installation of an application

You can enable the **Uninstall incompatible applications automatically** option when you configure remote installation of a security application in the Protection deployment wizard. When this option is enabled, Kaspersky Security Center Linux [removes incompatible applications before installing a security application on a managed device](#).

### Removing incompatible applications through a dedicated task

To remove incompatible applications, [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.

## Removing applications or software updates remotely

You can remove applications or software updates on managed devices that run Linux remotely only by using Network Agent.

*To remove applications or software updates remotely from selected devices:*

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

2. Click **Add**.

The New task wizard starts. Proceed through the wizard by using the **Next** button.

3. In the **Application** drop-down list, select Kaspersky Security Center.

4. In the **Task type** list, select the **Uninstall application remotely** task type.

5. In the **Task name** field, specify the name of the new task.

A task name cannot be more than 100 characters long and cannot include any special characters ("\*<>?\;|).

6. Select the [devices to which the task will be assigned](#).

Go to the next step of the wizard.

7. Select what kind of software you want to remove, and then select specific applications, updates, or patches that you want to remove:

- [Uninstall managed application](#) 

A list of Kaspersky applications is displayed. Select the application that you want to remove.

- [Uninstall application from applications registry](#) 



By default, Network Agents send the Administration Server information about the applications installed on the managed devices. The list of installed applications is stored in the applications registry.

To select an application from the applications registry:

- a. Click the **Application to uninstall** field, and then select the application that you want to remove.
- b. Specify the uninstallation options:

- **Uninstallation mode** 

Select how you want to remove the application:

- **Define uninstallation command automatically**

If the application has an uninstallation command defined by the application vendor, Kaspersky Security Center Linux uses this command. We recommend that you select this option.

- **Specify uninstallation command**

Select this option if you want to specify your own command for the application uninstallation.

We recommend that you first try to remove the application by using the **Define uninstallation command automatically** option. If the uninstallation through the automatically defined command fails, then use your own command.

Type an installation command into the field, and then specify the following option:

- **Use this command for uninstallation only if the default command was not autodetected** 

Kaspersky Security Center Linux checks whether or not the selected application has an uninstallation command defined by the application vendor. If the command is found, Kaspersky Security Center Linux will use it instead of the command specified in the **Command for application uninstallation** field.

We recommend that you enable this option.

- **Perform restart after successful application uninstallation** 

If the application requires the operating system to be restarted on the managed device after successful uninstallation, the operating system is restarted automatically.

- **Uninstall the specified application update, patch, or third-party application** 

A list of updates, patches, and third-party applications is displayed. Select the item that you want to remove.

The displayed list is a general list of applications and updates, and it does not correspond to the applications and updates installed on the managed devices. Before selecting an item, we recommend that you ensure that the application or update is installed on the devices defined in the task scope. You can view the list of devices on which the application or update is installed, via the properties window.

*To view the list of devices:*

- a. Click the name of the application or update.

The properties window opens.

- b. Open the **Devices** section.

You can also view the list of installed applications and updates in the [device properties window](#).

8. Specify how client devices will download the Uninstallation utility:

- [Using Network Agent](#) ?

The files are delivered to client devices by Network Agent installed on those client devices.

If this option is disabled, the files are delivered using the Linux operating system tools.

We recommend that you enable this option if the task has been assigned to devices that have Network Agents installed.

- [Using operating system resources through Administration Server](#) ?

The option is obsolete. Use the **Using Network Agent** or **Using operating system resources through distribution points** option instead.

The files are transmitted to client devices by using the Administration Server operating system tools. You can enable this option if no Network Agent is installed on the client device, but the client device is on the same network as the Administration Server.

- [Using operating system resources through distribution points](#) ?

The files are transmitted to client devices by using operating system tools through distribution points. You can enable this option if there is at least one distribution point on the network.

If the **Using Network Agent** option is enabled, the files are delivered by using operating system tools only if Network Agent tools are unavailable.

- [Maximum number of concurrent downloads](#) ?

The maximum allowed number of client devices to which Administration Server can simultaneously transmit the files. The larger this number, the faster the application will be uninstalled, but the load on Administration Server is higher.

- [Maximum number of uninstallation attempts](#) ?

If, when running the *Uninstall application remotely* task, Kaspersky Security Center Linux fails to uninstall an application on a managed device within the number of installer runs specified by the parameter, Kaspersky Security Center Linux stops delivering the Uninstallation utility to this managed device and does not start the installer on the device anymore.

The **Maximum number of uninstallation attempts** parameter allows you to save the resources of the managed device, as well as reduce traffic (uninstallation, MSI file run, and error messages).

Recurring task start attempts may indicate a problem on the device and which prevents uninstallation. The administrator should resolve the problem within the specified number of uninstallation attempts and then restart the task (manually or by a schedule).

If uninstallation is not achieved eventually, the problem is considered unresolvable and any further task starts are seen as costly in terms of unnecessary consumption of resources and traffic.

When the task is created, the attempts counter is set to 0. Each run of the installer that returns an error on the device increments the counter reading.

If the number of attempts specified in the parameter has been exceeded and the device is ready for application uninstallation, you can increase the value of the **Maximum number of uninstallation attempts** parameter and start the task to uninstall the application. Alternatively, you can create a new *Uninstall application remotely* task.

- [Verify operating system type before downloading](#) 

Before transmitting the files to client devices, Kaspersky Security Center Linux checks if the Installation utility settings are applicable to the operating system of the client device. If the settings are not applicable, Kaspersky Security Center Linux does not transmit the files and does not attempt to install the application. For example, to install some application to devices of an administration group that includes devices running various operating systems, you can assign the installation task to the administration group, and then enable this option to skip devices that run an operating system other than the required one.

Go to the next step of the wizard.

## 9. Specify the operating system restart settings:

- [Do not restart the device](#) 

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- [Restart the device](#) 

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- [Prompt user for action](#) 

The restart reminder is displayed on the screen of the client device, prompting the user to restart it manually. Some advanced settings can be defined for this option: text of the message for the user, the message display frequency, and the time interval after which a restart will be forced (without the user's confirmation). This option is most suitable for workstations where users must be able to select the most convenient time for a restart.

By default, this option is selected.

- **Repeat prompt every (min)**
- **Restart after (min)**
- **[Force closure of applications in blocked sessions](#)** ⓘ

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

Go to the next step of the wizard.

10. If necessary, add the accounts that will be used to start the remote uninstallation task:

- **[No account required \(Network Agent installed\)](#)** ⓘ

If this option is selected, you do not have to specify the account under which the application installer will be run. The task will run under the account under which the Administration Server service is running.

If Network Agent has not been installed on client devices, this option is not available.

- **[Account required \(Network Agent is not used\)](#)** ⓘ

Select this option if Network Agent is not installed on the devices for which you assign the *Uninstall application remotely* task.

Specify the user account under which the application installer will be run. Click the **Add** button, select **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.

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 will be created with the default settings. You can modify the default settings later.

12. Click the **Finish** button.

The wizard creates the task. If you enabled the **Open task details when creation is complete** option, the task properties window automatically opens. In this window, you can specify the general task settings and, if required, change the settings specified during task creation.

You can also open the task properties window by clicking the name of the created task in the list of tasks.

The task is created, configured, and displayed in the list of tasks at **Assets (Devices) → Tasks**.

13. To run the task, select it in the task list, and then click the **Start** button.

You can also set a task start schedule on the **Schedule** tab of the task properties window.

For a detailed description of scheduled start settings, refer to the [general task settings](#).

After the task is completed, the selected application is removed from the selected devices.

## Preparing a device running SUSE Linux Enterprise Server 15 for installation of Network Agent

*To install Network Agent on a device with the SUSE Linux Enterprise Server 15 operating system:*

Before the Network Agent installation, run the following command:

```
$ sudo zypper install insserv-compat
```

This enables you to install the `insserv-compat` package and configure Network Agent properly.

Run the `rpm -q insserv-compat` command to check whether the package is already installed.

If your network includes a lot of devices running SUSE Linux Enterprise Server 15, you can use the special software for configuring and managing the company infrastructure. By using this software, you can automatically install the `insserv-compat` package on all necessary devices at once. For example, you can use Puppet, Ansible, Chef, you can make your own script—use any method that is convenient for you.

If the device does not have the GPG signing keys for SUSE Linux Enterprise, you may encounter the following warning: `Package header is not signed!` Select the `i` option to ignore the warning.

After preparing the SUSE Linux Enterprise Server 15 device, [deploy and install Network Agent](#).

## Preparing a Windows device for remote installation. Riprep utility

Remote installation of the application on the client device may return an error for the following reasons:

- The task has already been successfully performed on this device. In this case, the task does not have to be performed again.
- When a task was started, the device was shut down. In this case, turn on the device and restart the task.

- There is no connection between the Administration Server and the Network Agent installed on the client device. To determine the cause of the problem, use the utility designed for remote diagnostics of client devices (klactgui).
- If Network Agent is not installed on the device, the following problems may occur during remote installation:
  - The client device has **Disable simple file sharing** enabled.
  - The Server service is not running on the client device.
  - The required ports are closed on the client device.
  - The account that is used to perform the task has insufficient privileges.

To solve problems that occur during installation of the application on a client device without Network Agent installed, you can use the utility designed to prepare devices for remote installation (riprep).

Use the riprep utility to prepare Windows a device for remote installation. To download the utility, click this link: <https://media.kaspersky.com/utilities/CorporateUtilities/KSC/riprep.exe>

The utility used to prepare a device for remote installation does not run on Microsoft Windows XP Home Edition.

## Preparing a Windows device for remote installation in interactive mode

*To prepare a Windows device for remote installation in interactive mode:*

1. Run the riprep.exe file on a client device.
2. In the main window of the remote installation preparation utility, select the following options:
  - **Disable simple file sharing**
  - **Start the Administration Server service**
  - **Open ports**
  - **Add an account**
  - **Disable User Account Control (UAC)** (only available for devices running Microsoft Windows Vista, Microsoft Windows 7, or Microsoft Windows Server 2008)
3. Click the **Start** button.

The stages of device preparation for remote installation are shown in the lower part of the utility's main window.

If you selected the **Add an account** option, when an account is created you will be prompted to enter the account name and password. This will create a local account belonging to the local administrators' group.

If you selected the **Disable User Account Control (UAC)** option, an attempt to disable User Account Control will be made even if UAC was disabled before the utility was started. After UAC is disabled, you will be prompted to restart the device.

## Preparing a Windows device for remote installation in silent mode

*To prepare a Windows device for remote installation in silent mode:*

Run the `riprep.exe` file on the client device from the command line with the requisite set of keys.

Utility command line syntax:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Descriptions of the keys:

- `-silent`—Starts the utility in silent mode.
- `-cfg CONFIG_FILE`—Defines the utility configuration, where `CONFIG_FILE` is the path to the configuration file (a file with the `.ini` extension).
- `-tl traceLevel`—Defines the trace level, where `traceLevel` is a number from 0 to 5. If no key is specified, the value 0 is used.

You can perform the following tasks by starting the utility in silent mode:

- Disabling the simple sharing of files
- Starting the Server service on the client device
- Opening the ports
- Creating a local account
- Disabling User Account Control (UAC)

You can specify the parameters for device preparation for remote installation in the configuration file specified in the `-cfg` key. To define these parameters, add the following information to the configuration file:

- In the `Common` section, specify the tasks to be performed:
  - `DisableSFS`—Disable the simple sharing of files (0 —the task is disabled; 1 —the task is enabled).
  - `StartServer`—Start the Server service (0 —the task is disabled; 1 —the task is enabled).
  - `OpenFirewallPorts`—Open the necessary ports (0 —the task is disabled; 1 —the task is enabled).
  - `DisableUAC`—Disable User Account Control (UAC) (0 —the task is disabled; 1 —the task is enabled).
  - `RebootType`—Define behavior if restart of device is required when UAC is disabled. You can use the following values:
    - 0—Never restart the device.
    - 1—Restart the device, if UAC was enabled before starting the utility.
    - 2—Force restart, if UAC was enabled before starting the utility.

- 4—Always restart the device.
- 5—Always restart the device with force.
- In the UserAccount section, specify the account name (user) and its password (Pwd).

Sample context of the configuration file:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1
[UserAccount]
user=Admin
Pwd=Pass123
```

After the utility completes, the following files will be created in the utility start folder:

- riprep.txt—Operation report, in which phases of the utility operation are listed with reasons for these operations.
- riprep.log—Trace file (created if the tracing level is set above 0).



# Licensing

This section provides the following information:

- General concepts related to Kaspersky Security Center Linux licensing
- Instructions on license management of managed Kaspersky applications

## About licensing of Kaspersky Security Center Linux

This section describes general concepts related to Kaspersky Security Center Linux licensing.

## About the End User License Agreement

*The End User License Agreement* (License Agreement or EULA) is a binding agreement between you and AO Kaspersky Lab stipulating the terms under which you may use the application.

Carefully read the License Agreement before you start using the application.

Kaspersky Security Center Linux and its components, for example, Network Agent, have their own EULA.

You can view the terms of the End User License Agreement for Kaspersky Security Center Linux by using the following methods:

- During installation of Kaspersky Security Center.
- By reading the license.txt document included in the Kaspersky Security Center distribution kit.
- By reading the license.txt document in the Kaspersky Security Center installation folder.
- By downloading the license.txt file from the [Kaspersky website](#).

You can view the terms of the End User License Agreement for Network Agent for Linux by using the following methods:

- While downloading the Network Agent distribution package from the Kaspersky web servers.
- During installation of Network Agent for Linux.
- By reading the license.txt document included in the Network Agent for Linux distribution package.
- By reading the license.txt document in the Network Agent for Linux installation folder.
- By downloading the license.txt file from the [Kaspersky website](#).

You accept the terms of the End User License Agreement by confirming that you agree with the End User License Agreement when installing the application. If you do not accept the terms of the License Agreement, cancel the application installation and do not use the application.

## About the license

A *license* is a time-limited right to use Kaspersky Security Center Linux, granted under the terms of the signed License Contract (End User License Agreement).

The scope of services and validity period depend on the license under which the application is used.

The following license types are provided:

- *Trial*

A free license intended for trying out the application. A trial license usually has a short term.

When a trial license expires, all Kaspersky Security Center Linux features become disabled. To continue using the application, you need to purchase a commercial license.

You can use the application under a trial license for only one trial period.

- *Commercial*

A paid license.

When a commercial license expires, key features of the application become disabled. To continue using Kaspersky Security Center, you must renew your commercial license. After a commercial license expires, you cannot continue using the application and must remove it from your 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 you receive along with a key file or an activation code.

A license certificate contains the following information about the license provided:

- License key or order number
- Information about the user who has been 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)
- License validity start date
- License expiration date or license term
- License type

## About the license key

A *license key* is a sequence of bits that you can apply to activate and then use the application in accordance with the terms of the End User License Agreement. License keys are generated by Kaspersky specialists.

You can add a license key to the application using one of the following methods: by applying a *key file* or by entering an *activation code*. The license key is displayed in the application interface as a unique alphanumeric sequence after you add it to the application.

The license key may be blocked by Kaspersky in case the terms of the License Agreement have been violated. If the license key has been blocked, you need to add another one if you want to use the application.

A license key may be active or additional (or reserve).

An *active license key* is a license key that is currently used by the application. An active license key can be added for a trial or commercial license. The application cannot have more than one active license key.

An *additional (or reserve) license key* is a license key that entitles the user to use the application, but is not currently in use. The additional license key automatically becomes active when the license associated with the current active license key expires. An additional license key can be added only if an active license key has already been added.

A license key for a trial license can be added as an active license key. A license key for a trial license cannot be added as an additional license key.

## Viewing the Privacy Policy

The Privacy Policy is available online at <https://www.kaspersky.com/products-and-services-privacy-policy>.

The Privacy Policy is also available offline:

- You can read the Privacy Policy before [Installing Kaspersky Security Center Linux](#).
- The Privacy Policy text is included in the license.txt file, in the Kaspersky Security Center Linux installation folder.
- The privacy\_policy.txt file is available on a managed device, in the Network Agent installation folder.
- You can unpack the privacy\_policy.txt file from the Network Agent distribution package.

## Kaspersky Security Center licensing options

Kaspersky Security Center is delivered as a part of Kaspersky applications for protection of corporate networks. You can also download it from [Kaspersky website](#).

Using Kaspersky Security Center, you can do the following:

- Create a hierarchy of Administration Servers to manage the organization's network, as well as networks at remote offices or client organizations.  
The *client organization* is an organization whose anti-virus protection is ensured by the service provider.
- Create a hierarchy of administration groups to manage a selection of client devices as a whole.
- Manage an anti-virus protection system built based on Kaspersky applications.

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

## About the key file

A *key file* is a file with the .key extension provided to you by Kaspersky. Key files are designed to activate the application by adding a license key.

You receive a key file at the email address that you provided when you bought Kaspersky Security Center or ordered the trial version of Kaspersky Security Center.

You do not need to connect to Kaspersky activation servers in order to activate the application with a key file.

You can restore a key file if it has been accidentally deleted. You may need a key file to register a Kaspersky CompanyAccount, for example.

To restore your key file, perform any of the following actions:

- Contact the license seller.
- Receive a key file through [Kaspersky website](#) <sup>2</sup> by using your available activation code.

## About data provision

### Data processed locally

Kaspersky Security Center Linux is designed for centralized execution of basic administration and maintenance tasks on an organization's network. Kaspersky Security Center Linux provides the administrator with access to detailed information about the organization's network security level; Kaspersky Security Center Linux lets an administrator configure all the components of protection based on Kaspersky applications. Kaspersky Security Center Linux performs the following main functions:

- Detecting devices and their users on the organization's network
- Creating a hierarchy of administration groups for device management

- Installing Kaspersky applications on devices
- Managing the settings and tasks of installed applications
- Activating Kaspersky applications on devices
- Managing user accounts
- Viewing information about the operation of Kaspersky applications on devices
- Viewing reports

To perform its main functions Kaspersky Security Center Linux can receive, store, and process the following information:

- Information about the devices on the organization's network received through scanning of Active Directory or Samba domain controllers or through scanning of IP intervals. Administration Server gets data independently or receives data from Network Agent.
- Information from Active Directory and Samba about organizational units, domains, users, and groups. Administration Server gets data by itself or receives data from Network Agent assigned to work as a distribution point.
- Details of managed devices. Network Agent transfers the data listed below from the device to Administration Server. The user enters the display name and description of the device in the Kaspersky Security Center Web Console interface:
  - Technical specifications of the managed device and its components required for device identification: device display name and description, Windows domain name and type (for devices belonging to a Windows domain), device name in Windows environment (for devices belonging to a Windows domain), DNS domain and DNS name, IPv4 address, IPv6 address, network location, MAC address, operating system type, whether the device is a virtual machine together with hypervisor type, and whether the device is a dynamic virtual machine as part of VDI.
  - Other specifications of managed devices and their components required for audit of managed devices: operating system architecture, operating system vendor, operating system build number, operating system release ID, operating system location folder, if the device is a virtual machine—the virtual machine type, name of the virtual Administration Server that manages the device.
  - Details of actions on managed devices: date and time of the last update, time the device was last visible on the network, restart waiting status, and time the device was turned on.
  - Details of device user accounts and their work sessions.
- Data received by running remote diagnostics on a managed device: trace files, system information, details of Kaspersky applications installed on the device, dump files, event logs, the results of running the diagnostic scripts received from Kaspersky Technical Support.
- Distribution point operation statistics if the device is a distribution point. Network Agent transfers data from the device to Administration Server.
- Distribution point settings entered by the User in Kaspersky Security Center Web Console.
- Details of Kaspersky applications installed on the device. The managed application transfers data from the device to Administration Server through Network Agent:

- Settings of Kaspersky applications installed on the managed device: Kaspersky application name and version, status, real-time protection status, last device scan date and time, number of threats detected, number of objects that failed to be disinfected, availability and status of the application components, details of Kaspersky application settings and tasks, information about the current and reserve license keys, application installation date and ID.
- Application operation statistics: events related to the changes in the status of Kaspersky application components on the managed device and to the performance of tasks initiated by the application components.
- Device status defined by the Kaspersky application.
- Tags assigned by the Kaspersky application.
- Data contained in events from Kaspersky Security Center Linux components and Kaspersky managed applications. Network Agent transfers data from the device to Administration Server.
- Settings of Kaspersky Security Center Linux components and Kaspersky managed applications presented in policies and policy profiles. The User enters data in the Kaspersky Security Center Web Console interface.
- Task settings of Kaspersky Security Center Linux components and Kaspersky managed applications. The User enters data in the Kaspersky Security Center Web Console interface.
- Data processed by the System management feature. Network Agent transfers from the device to Administration Server the following information:
  - Information about the hardware detected on managed devices (Hardware registry).
  - Information about the software installed on managed devices (Software registry). The software can be compared with the information about the executable files detected on the devices by the Application Control function.
- User categories of applications. The User enters data in the Kaspersky Security Center Web Console interface.
- Details of executable files detected on managed devices by the Application Control feature. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Information about encrypted Windows-based devices and the encryption status. The managed application transfers data from the device to Administration Server through Network Agent.
- Details of data encryption errors on Windows-based devices performed using the Data encryption feature of Kaspersky applications. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Details of files placed in Backup. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Details of files placed in Quarantine. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Details of files requested by Kaspersky specialists for detailed analysis. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.

- Details of external devices (memory units, information transfer tools, information hardcopy tools, and connection buses) installed or connected to the managed device and detected by the Device Control feature. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Information about encrypted devices and the encryption status. A managed application transfers data from the device to Administration Server through Network Agent.
- Information about data encryption errors on the devices. The encryption is performed by the Encryption data function of Kaspersky applications. A managed application transfers data from the device to Administration Server through Network Agent. The full list of data is provided in the Online Help of the corresponding application.
- List of managed programmable logic controllers (PLCs). The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Data required for creation of a threat development chain. The managed application transfers data from the device to Administration Server through Network Agent. A complete list of data is provided in the Help files of the corresponding application.
- Details of the entered activation codes and key files. The User enters data in the Administration Console or Kaspersky Security Center Web Console interface.
- User accounts: name, description, full name, email address, main phone number, and password. The User enters data in the Kaspersky Security Center Web Console interface.
- Revision history of management objects. The User enters data in the Kaspersky Security Center Web Console interface.
- Registry of deleted management objects. The User enters data in the Kaspersky Security Center Web Console interface.
- Installation packages created from the file, as well as installation settings. The User enters data in the Kaspersky Security Center Web Console interface.
- Data required for the display of announcements from Kaspersky in Kaspersky Security Center Web Console. The User enters data in the Kaspersky Security Center Web Console interface.
- Data required for the functioning of plug-ins of managed applications in Kaspersky Security Center Web Console and saved by the plug-ins in the Administration Server database during their routine operation. The description and ways of providing the data are provided in the Help files of the corresponding application.
- Kaspersky Security Center Web Console user settings: localization language and theme of the interface, Monitoring panel display settings, information about the status of notifications (Already read / Not yet read), status of columns in spreadsheets (Show / Hide), Training mode progress. The User enters data in the Kaspersky Security Center Web Console interface.
- Certificate for secure connection of managed devices to the Kaspersky Security Center Linux components. The User enters data in the Kaspersky Security Center Web Console interface.
- Information on which Kaspersky legal agreement terms have been accepted by the user.
- The Administration Server data that the User enters in the Kaspersky Security Center Web Console or program interface Kaspersky Security Center OpenAPI.
- Any data that the User enters in the Kaspersky Security Center Web Console interface.

The data listed above can be present in Kaspersky Security Center Linux if one of the following methods is applied:

- The User enters data in the Kaspersky Security Center Web Console interface.
- Network Agent automatically receives data from the device and transfers it to Administration Server.
- Network Agent receives data retrieved by the Kaspersky managed application and transfers it to Administration Server. The lists of data processed by Kaspersky managed applications are provided in the Help files for the corresponding applications.
- Administration Server gets the information about the networked devices by itself or receives data from Network Agent assigned to work as a distribution point.

The listed data is stored in the Administration Server database. User names and passwords are stored in encrypted form.

All data processed locally can be transferred to Kaspersky only through dump files, trace files, or log files of Kaspersky Security Center Linux components, including log files created by installers and utilities.

The dump files, trace files, or log files of Kaspersky Security Center Linux components contain arbitrary data of Administration Server, Network Agent, and Kaspersky Security Center Web Console. The files may contain personal or confidential data. The dump files, trace files, or log files are stored on the devices in an unencrypted form. The dump files, trace files, or log files are not transferred to Kaspersky automatically, but an administrator may transfer those files to Kaspersky manually by request from Technical Support to resolve issues related to Kaspersky Security Center Linux performance.

Kaspersky protects any information received in accordance with law and applicable Kaspersky rules. Data is transmitted over a secure channel.

Following the links in the Administration Console or Kaspersky Security Center Web Console, the User agrees to the automatic transfer of the following data:

- Kaspersky Security Center Linux code
- Kaspersky Security Center Linux version
- Kaspersky Security Center Linux localization
- License ID
- License type
- Whether the license was purchased through a partner

The list of data provided via each link depends on the purpose and location of the link.

Kaspersky uses the received data in anonymized form and for general statistics only. Summary statistics are generated automatically from the originally received information and do not contain any personal or confidential data. As soon as new data is accumulated, the previous data is wiped (once a year). Summary statistics are stored indefinitely.

## About the subscription



*Subscription to Kaspersky Security Center Linux* is an order for use of the application under the selected settings (subscription expiration date, number of protected devices). You can register your subscription to Kaspersky Security Center Linux with your service provider (for example, your internet provider). A subscription can be renewed manually or in automatic mode; also, you can cancel it.

A subscription can be limited (for example, one-year) or unlimited (with no expiration date). To continue using Kaspersky Security Center after a limited subscription expires, you must renew it. An unlimited subscription is renewed automatically if it has been prepaid to the service provider in due dates.

When a limited subscription expires, you may be provided a grace period for renewal during which the application continues to function. The availability and duration of the grace period is defined by the service provider.

To use Kaspersky Security Center Linux under subscription, you must apply the activation code received from the service provider.

You can apply a different activation code for Kaspersky Security Center Linux only after your subscription expires or when you cancel it.

Depending on the service provider, the set of possible actions for subscription management may vary. The service provider might not provide a grace period for subscription renewal and so the application loses its functionality.

Activation codes purchased under subscription cannot be used for activating earlier versions of Kaspersky Security Center.

When the application is used under subscription, Kaspersky Security Center Linux automatically attempts to access the activation server at specified time intervals until the subscription expires. If access to the server using system DNS is not possible, the application uses [public DNS servers](#). You can renew your subscription on the service provider's website.

## Activating Kaspersky Security Center Linux

You can activate licensed features to use additional functionality of Kaspersky Security Center Linux. There are two ways to accomplish this task: use the [Administration Server Quick Start Wizard](#) or the Administration Server properties.

*To activate licensed features of Kaspersky Security Center Linux:*

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 **License keys** section.
3. Under **Current license**, click the **Select** button.
4. In the window that opens, select the license key that you want to use to activate Kaspersky Security Center Linux. If the license key is not listed, click the **Add new license key** button, and then specify a new license key.
5. If necessary, you can also add a [reserve license key](#) 🗒️. To do this, under **Reserve license key**, click the **Select** button, and then select an existing license key or add a new one. Note that you cannot add a reserve license key if there is no active license key.
6. Click the **Save** button.

## Licensing of managed Kaspersky applications

This section describes the features of Kaspersky Security Center related to working with the license keys of managed Kaspersky applications.

Kaspersky Security Center Linux allows you to perform centralized distribution of license keys for Kaspersky applications on client devices, monitor their use, and renew licenses.

When adding a license key using Kaspersky Security Center, the settings of the license key are saved on the Administration Server. Based on this information, the application generates a license key usage report and notifies the administrator of license expirations and violation of license restrictions that are set in the properties of license keys. You can configure notifications of the use of license keys within the Administration Server settings.

## Licensing of managed applications

The Kaspersky applications installed on managed devices must be licensed by applying a key file or activation code to each of the applications. A key file or activation code can be deployed in the following ways:

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

You can add a new active or reserve license key by any of the methods listed above. A Kaspersky application uses an active key at the current moment and stores a reserve key to apply after the active key expires. The application for which you add a license key defines whether the key is active or reserve. The key definition does not depend on the method that you use to add a new license key.

### Automatic deployment

If you use different managed applications and you have to deploy a specific key file or activation code to devices, opt for other ways of deploying that activation code or key file.

Kaspersky Security Center allows you to automatically deploy available license keys to devices. For example, three license keys are stored in the Administration Server repository. You have enabled the **Automatically distributed license key** option for all three license keys. A Kaspersky security application—for example, Kaspersky Endpoint Security for Linux—is installed on the organization's devices. A new device is discovered to which a license key must be deployed. The application determines, for instance, that two of the license keys from the repository can be deployed to the device: license key named *Key\_1* and license key named *Key\_2*. One of these license keys is deployed to the device. In this case, it cannot be predicted which of the two license keys will be deployed to the device because automatic deployment of license keys does not provide for any administrator activity.

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

Before deployment, the key file or activation code must be added to the Administration Server repository.

How-to instructions:

- [Adding a license key to the Administration Server repository](#)
- [Automatic distribution of a license key](#)

Note that an automatically distributed license key may not be displayed in the virtual Administration Server repository in the following cases:

- The license key is not valid for the application.
- The virtual Administration Server does not have managed devices.
- The license key has already been used for devices managed by another virtual Administration Server and the limit on the number of devices has been reached.

## Adding a key file or activation code to the installation package of a managed application

For security reasons, this option is not recommended. A key file or activation code added to an installation package may be compromised.

If you install a managed application using an installation package, you can specify an activation code or key file in this installation package or in the policy of the application. The license key will be deployed to managed devices at the next synchronization of the device with the Administration Server.

How-to instructions: [Adding a license key to an installation package](#)

## Deployment through the Add license key task for a managed application

If you opt for using the Add license key task for a managed application, you can select the license key that must be deployed to devices and select the devices in any convenient way—for example, by selecting an administration group or a device selection.

Before deployment, the key file or activation code must be added to the Administration Server repository.

How-to instructions:

- [Adding a license key to the Administration Server repository](#)
- [Deploying a license key to client devices](#)

## Adding an activation code or a key file manually to the devices

You can activate the installed Kaspersky application locally, by using the tools provided in the application interface. Please refer to the documentation of the installed application.

## Adding a license key to the Administration Server repository

To add a license key to the Administration Server repository:

1. In the main menu, go to **Operations** → **Licensing** → **Kaspersky licenses**.
2. Click the **Add** button.
3. Choose what you want to add:
  - **Add key file**  
Click the **Select key file** button and browse to the .key file that you want to add.
  - **Enter activation code**  
Specify the activation code in the text field and click the **Send** button.
4. Click the **Close** button.

The license key or several license keys are added to the Administration Server repository.

## Deploying a license key to client devices

Kaspersky Security Center Web Console allows you to distribute a license key to client devices [automatically](#) or through the add key task.

Before deployment, [add the license key to the Administration Server repository](#).

To distribute a license key to client devices through the add key task:

1. In the main menu, go to **Assets (Devices)** → **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 **Add key** task.
5. In the **Task name** field, specify the name of the new task.
6. Select the [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 add key 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, enable the **Use as a reserve key** option if you want to use this key as a reserve key.

In this case, a reserve key is applied after the active key expires.

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 will be 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 Security Center Linux allows automatic distribution of license keys to managed devices if they are located in the license keys repository on the Administration Server.

*To distribute a license key to managed devices automatically:*

1. In the main menu, go to **Operations** → **Licensing** → **Kaspersky 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, select the **Automatically distribute license key to managed devices** check box.
4. Click the **Save** button.

The license key will be automatically distributed to all compatible devices.

License key distribution is performed by means of Network Agent. No license key distribution tasks are created for the application.

During automatic distribution of a license key, the licensing limit on the number of devices is taken into account. The licensing limit is set in the properties of the license key. If the licensing 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 select the **Automatically distribute license key to managed devices** check box in the license key properties window, a license key is distributed on your network immediately. If you do not select this option, you can manually distribute a license key later.

## Viewing information about license keys in use

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

In the main menu, go to **Operations** → **Licensing** → **Kaspersky licenses**.

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

*To view detailed information about a license key:*

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

*To view which license keys are deployed to a specific client device:*

1. In the main menu, go to **Assets (Devices) → Managed devices**.
2. Click the name of the required device.
3. In the device properties window that opens, select the **Applications** tab.
4. Click the name of the application for which you want to view the information about the license key.
5. In the application properties window that opens, select the **General** tab, and then open the **License** section.

The main information about the active and reserve license keys is displayed.

To define the up-to-date settings of virtual Administration Server license keys, the Administration Server sends a request to Kaspersky activation servers at least once per day. If access to the servers using system DNS is not possible, the application uses [public DNS servers](#).

## Events of the licensing limit exceeded

Kaspersky Security Center Linux allows you to get information about events when some licensing limits are exceeded by Kaspersky applications installed on client devices.

The importance level of such events when a licensing restriction is exceeded is defined according to the following rules:

- If the currently used units covered by a single license constitute 90% to 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% to 110% of the total number of units covered by the license, the event is published with the **Warning** importance level.
- If the number of currently used units covered by a single license exceeds 110% of the total number of units covered by the license, the event is published with the **Critical event** importance level.

## Deleting a license key from the repository

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

To delete a key file or activation code from the Administration Server repository:

1. Check that Administration Server does not use a key file or activation code that you want to delete. If the Administration Server does, you cannot delete the key. To perform the check:
  - a. In the main menu, click the settings icon (⚙️) next to the Administration Server.  
The Administration Server properties window opens.
  - b. On the **General** tab, select the **License keys** section.
  - c. If the required key file or activation code is displayed in the section that opens, click the **Remove active license key** button, and then confirm the operation. After that, the Administration Server does not use the deleted license key, but the key remains in the Administration Server repository. If the required key file or activation code is not displayed, the Administration Server does not use it.
2. In the main menu, go to **Operations** → **Licensing** → **Kaspersky licenses**.
3. Select the required key file or activation code, and then click the **Delete** button.

The selected key file or activation code is deleted from the repository.

You can [add](#) a deleted license key again or add a new license key.

## Revoking consent with an End User License Agreement

If you decide to stop protecting some of your client devices, you can revoke the End User License Agreement (EULA) for any managed Kaspersky application. You must uninstall the selected application before revoking its EULA.

To revoke a EULA for managed Kaspersky applications:

1. Open the Administration Server properties window and on the **General** tab select the **End User License Agreements** section.  
A list of EULAs—accepted upon creation of installation packages, at the seamless installation of updates, or upon deployment of Kaspersky Security for Mobile—is displayed.
2. In the list, select the EULA that you want to revoke.  
You can view the following properties of the EULA:
  - Date when the EULA was accepted
  - Name of the user who accepted the EULA
3. Click the acceptance date of any EULA to open its properties window that displays the following data:
  - Name of the user who accepted the EULA
  - Date when the EULA was accepted
  - Unique identifier (UID) of the EULA
  - Full text of the EULA



- List of objects (installation packages, seamless updates, mobile apps) linked to the EULA, and their respective names and types

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

If there exist any objects (installation packages and their respective tasks) that prevent the EULA from being revoked, the corresponding notification is displayed. You cannot proceed with revocation until you delete these objects.

In the window that opens, you are informed that you must first uninstall the Kaspersky application corresponding to the EULA.

5. Click the button to confirm revocation.

The EULA is revoked. It is no longer displayed in the list of License Agreements in the **End User License Agreements** section. The EULA properties window closes; the application is no longer installed.

## Renewing licenses for Kaspersky applications

You can renew a Kaspersky application license that has expired or is about to expire (in less than 30 days).

*To renew an expired license or a license that is about to expire:*

1. Do either of the following:

- In the main menu, go to **Operations** → **Licensing** → **Kaspersky licenses**.
- In the main menu, go to **Monitoring & reporting** → **Dashboard**, and then click the **View expiring licenses** link next to a notification.

The **Kaspersky licenses** window opens, where you can view and renew licenses.

2. Click the **Renew license** link next to the required license.

By clicking a license renewal link, you agree to transfer to Kaspersky the following information about Kaspersky Security Center Linux: its version, the localization you are using, the software license ID (that is, the ID of the license you are renewing), and whether you purchased the license via a partner company or not.

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

The license is renewed.

In Kaspersky Security Center Web Console, the notifications are displayed when a license is about to expire, according to the following schedule:

- 30 days before the expiration
- 7 days before the expiration
- 3 days before the expiration
- 24 hours before the expiration

- When a license has expired

## Using Kaspersky Marketplace to choose Kaspersky business solutions

**Marketplace** is a section in the main menu that enables you to view the entire range of Kaspersky business solutions, select the ones you need, and proceed to the purchase at the Kaspersky website. You can use filters to view only those solutions that fit your organization and the requirements for your information security system. When you select a solution, Kaspersky Security Center Linux redirects you to the related webpage at the Kaspersky website to learn more about that solution. Each webpage enables you to proceed to the purchase or contains instructions on the purchase process.

In the **Marketplace** section, you can filter Kaspersky solutions by using the following criteria:

- Number of devices (endpoints, servers, and other types of assets) that you want to protect:
  - 50–250
  - 250–1000
  - More than 1000
- Maturity level of your organization's information security team:
  - **Foundations**  
This level is typical for enterprises that only have an IT team. The maximum possible number of threats is blocked automatically.
  - **Optimum**  
This level is typical for enterprises that have a specific IT security function within the IT team. At this level, companies require solutions that enable them to counter commodity threats and threats that circumvent existing preventive mechanisms.
  - **Expert**  
This level is typical for enterprises with complex and distributed IT environments. The IT security team is mature or the company has an SOC (Security Operations Center) team. The required solutions enable the companies to counter complex threats and targeted attacks.
- Types of assets that you want to protect:
  - **Endpoints:** workstations of employees, physical and virtual machines, embedded systems
  - **Servers:** physical and virtual servers
  - **Cloud:** public, private, or hybrid cloud environments; cloud services
  - **Network:** local area network, IT infrastructure
  - **Service:** security-related services provided by Kaspersky

*To find and purchase a Kaspersky business solution:*

1. In the main menu, go to **Marketplace**.

By default, the section displays all available Kaspersky business solutions.

2. To view only those solutions that suit your organization, select the required values in the filters.

3. Click the solution that you want to purchase or you want to learn more about.

You will be redirected to the solution webpage. You can follow the on-screen instructions to proceed to the purchase.

# Configuring Kaspersky applications

This section contains information about manual configuration of policies and tasks, about user roles, about building an administration group structure and hierarchy of tasks.

## Scenario: Configuring network protection

The quick start wizard creates policies and tasks with the default settings. These settings may turn out to be sub-optimal or even disallowed by an organization. Therefore, we recommend that you fine-tune these policies and tasks, and then create other policies and tasks if they are necessary for your network.

### Prerequisites

Before you start, make sure that you have done the following:

- [Installed Kaspersky Security Center Linux Administration Server](#)
- [Installed Kaspersky Security Center Web Console](#)
- Completed the Kaspersky Security Center Linux main installation scenario
- Completed the [quick start wizard](#) or manually created the following policies and tasks in the **Managed devices** administration group:
  - Policy of Kaspersky Endpoint Security
  - Group task for updating Kaspersky Endpoint Security
  - Policy of Network Agent

### Stages

Configuring network protection proceeds in stages:

#### 1 Setup and propagation of Kaspersky application policies and policy profiles

To configure and propagate settings for Kaspersky applications installed on the managed devices, you can use [two different security management approaches](#)—device-centric or user-centric. These two approaches can be combined.

#### 2 Configuring tasks for remote management of Kaspersky applications

Check the tasks created with the quick start wizard and fine-tune them, if necessary.

How-to instructions: [Setting up the group task for updating Kaspersky Endpoint Security](#)

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 during the operation of managed applications is transferred from a client device and registered in the Administration Server database. To reduce the load on the Administration Server, evaluate and limit the maximum number of events that can be stored in the database.

How-to instructions: [Setting the maximum number of events](#).

## Results

Upon completion of this scenario, your network will be protected by configuration of Kaspersky applications, tasks, and events received by the Administration Server:

- The Kaspersky applications are configured according to the policies and policy profiles.
- The applications are managed through a set of tasks.
- The maximum number of events that can be stored in the database is set.

When the network protection configuration is complete, you can proceed to [configure regular updates to Kaspersky databases and applications](#).

## About device-centric and user-centric security management approaches

You can manage security settings from the standpoint of device features and from the standpoint of user roles. The first approach is called *device-centric security management* and the second is called *user-centric security management*. To apply different application settings to different devices you can use either or both types of management in combination.

[Device-centric security management](#) enables you to apply different security application settings to managed devices depending on device-specific features. For example, you can apply different settings to devices allocated in different administration groups.

[User-centric security management](#) enables you to apply different security application settings to different user roles. You can create several user roles, assign an appropriate user role to each user, and define different application settings to the devices owned by users with different roles. For example, you may want to apply different application settings to devices of accountants and human resources (HR) specialists. As a result, when user-centric security management is implemented, each department—accounts department and HR department—has its own settings configuration for Kaspersky applications. A settings configuration defines which application settings can be changed by users and which are forcibly set and locked by the administrator.

By using user-centric security management you can apply specific application settings to individual users. This may be required when an employee has a unique role in the company or when you want to monitor security issues related to devices of a specific person. Depending on the role of this employee in the company, you can expand or limit the rights of this person to change application settings. For example, you might want to expand the rights of a system administrator who manages client devices in a local office.

You can also combine the device-centric and user-centric security management approaches. For example, you can configure a specific application policy for each administration group, and then create [policy profiles](#) for one or several user roles of your enterprise. In this case the policies and policy profiles are applied in the following order:

1. The policies created for device-centric security management are applied.
2. They are modified by the policy profiles according to the policy profile priorities.
3. The policies are modified by the [policy profiles associated with user roles](#).

# Policy setup and propagation: Device-centric approach

When you complete this scenario, the applications will be configured on all of the managed devices in accordance with the application policies and policy profiles that you define.

## Prerequisites

Before you start, make sure that you have [installed Kaspersky Security Center Linux Administration Server](#) and [Kaspersky Security Center Web Console](#). You might also want to consider [user-centric security management](#) as an alternative or additional option to the device-centric approach. Learn more about [two management approaches](#).

## Stages

The scenario of device-centric management of Kaspersky applications consists of the following steps:

### 1 Configuring application policies

Configure settings for Kaspersky applications installed on the managed devices by creating a [policy](#) for each application. The set of policies will be propagated to the client devices.

When you configure the protection of your network in quick start wizard, Kaspersky Security Center Linux creates the default policy for the following applications:

- Kaspersky Endpoint Security for Linux—for Linux-based client devices
- Kaspersky Endpoint Security for Windows—for Windows-based client devices

If you completed the configuration process by using this wizard, you do not have to create a new policy for this application.

If you have a hierarchical structure of several Administration Servers and/or administration groups, the secondary Administration Servers and child administration groups inherit the policies from the primary Administration Server by default. You can force the inheritance by the child groups and secondary Administration Servers to prohibit any modifications of the settings configured in the upstream policy. If you want only part of the settings to be forcibly inherited, you can lock them in the upstream policy. The rest unlocked settings will be available for modification in the downstream policies. The created hierarchy of policies will allow you to effectively manage devices in the administration groups.

How-to instructions: [Creating a policy](#)

### 2 Creating policy profiles (optional)

If you want devices within a single administration group to run under different policy settings, create [policy profiles](#) for those devices. A policy profile is a named subset of policy settings. This subset is distributed on target devices together with the policy, supplementing it under a specific condition called the *profile activation condition*. Profiles only contain settings that differ from the "basic" policy, which is active on the managed device.

By using profile activation conditions, you can apply different policy profiles, for example, to the devices having a specific hardware configuration or marked with specific [tags](#). Use tags to filter devices that meet specific criteria. For example, you can create a tag called *CentOS*, mark all devices running CentOS operating system with this tag, and then specify this tag as an activation condition for a policy profile. As a result, Kaspersky applications installed on all devices running CentOS will be managed by their own policy profile.

How-to instructions:

- [Creating a policy profile](#)

- [Creating a policy profile activation rule](#)

### 3 Propagating policies and policy profiles to the managed devices

By default, the Administration Server automatically synchronizes with managed devices every 15 minutes. During the synchronization, the new or changed policies and policy profiles are propagated to the managed devices. You can circumvent auto-synchronization and run the synchronization manually by using the Force synchronization command. When synchronization is complete, the policies and policy profiles are delivered and applied to the installed Kaspersky applications.

You can check whether the policies and policy profiles were delivered to a device. Kaspersky Security Center Linux specifies the delivery date and time in the properties of the device.

How-to instructions: [Forced synchronization](#)

## Results

When the device-centric scenario is complete, the Kaspersky applications are configured according to the settings specified and propagated through the hierarchy of policies.

The configured application policies and policy profiles will be applied automatically to the new devices added to the administration groups.

## Policy setup and propagation: User-centric approach

This section describes the scenario of user-centric approach to the centralized configuration of Kaspersky applications installed on the managed devices. When you complete this scenario, the applications will be configured on all of the managed devices in accordance with the application policies and policy profiles that you define.

### Prerequisites

Before you start, make sure that you have successfully [installed Kaspersky Security Center Linux Administration Server](#) and [Kaspersky Security Center Web Console](#), and completed the main deployment scenario. You might also want to consider [device-centric security management](#) as an alternative or additional option to the user-centric approach. Learn more about [two management approaches](#).

### Process

The scenario of user-centric management of Kaspersky applications consists of the following steps:

#### 1 Configuring application policies

Configure settings for Kaspersky applications installed on the managed devices by creating a policy for each application. The set of policies will be propagated to the client devices.

When you configure the protection of your network in quick start wizard, Kaspersky Security Center Linux creates the default policy for Kaspersky Endpoint Security. If you completed the configuration process by using this wizard, you do not have to create a new policy for this application.

If you have a hierarchical structure of several Administration Servers and/or administration groups, the secondary Administration Servers and child administration groups inherit the policies from the primary Administration Server by default. You can force the inheritance by the child groups and secondary Administration Servers to prohibit any modifications of the settings configured in the upstream policy. If you want only part of the settings to be forcibly inherited, you can [lock them in the upstream policy](#). The rest unlocked settings will be available for modification in the downstream policies. The created [hierarchy of policies](#) will allow you to effectively manage devices in the administration groups.

How-to instructions: [Creating a policy](#).

## 2 Specifying owners of the devices

Assign the managed devices to the corresponding users.

How-to instructions: [Assigning a user as a device owner](#)

## 3 Defining user roles typical for your enterprise

Think about different kinds of work that the employees of your enterprise typically perform. You must divide all employees in accordance with their roles. For example, you can divide them by departments, professions, or positions. After that you will need to create a user role for each group. Keep in mind that each user role will have its own policy profile containing application settings specific for this role.

## 4 Creating user roles

Create and configure a user role for each group of employees that you defined on the previous step or use the predefined user roles. The user roles will contain set of rights of access to the application features.

How-to instructions: [Creating a user role](#)

## 5 Defining the scope of each user role

For each of the created user roles, define users and/or security groups and administration groups. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.

How-to instructions: [Editing the scope of a user role](#)

## 6 Creating policy profiles

Create a [policy profile](#) for each user role in your enterprise. The policy profiles define which settings will be applied to the applications installed on users' devices depending on the role of each user.

How-to instructions: [Creating a policy profile](#)

## 7 Associating policy profiles with the user roles

Associate the created policy profiles with the user roles. After that: the policy profile becomes active for a user that has the specified role. The settings configured in the policy profile will be applied to the Kaspersky applications installed on the user's devices.

How-to instructions: [Associating policy profiles with roles](#)

## 8 Propagating policies and policy profiles to the managed devices

By default, Kaspersky Security Center Linux automatically synchronizes the Administration Server with the managed devices every 15 minutes. During the synchronization, the new or changed policies and policy profiles are propagated to the managed devices. You can circumvent auto-synchronization and run the synchronization manually by using the Force synchronization command. When synchronization is complete, the policies and policy profiles are delivered and applied to the installed Kaspersky applications.

You can check whether the policies and policy profiles were delivered to a device. Kaspersky Security Center Linux specifies the delivery date and time in the properties of the device.

How-to instructions: [Forced synchronization](#)



## Results

When the user-centric scenario is complete, the Kaspersky applications are configured according to the settings specified and propagated through the hierarchy of policies and policy profiles.

For a new user, you will have to create a new account, assign the user one of the created user roles, and assign the devices to the user. The configured application policies and policy profiles will be automatically applied to the devices of this user.

## Policies and policy profiles

In Kaspersky Security Center Web Console, you can create policies for Kaspersky applications. This section describes policies and policy profiles, and provides instructions for creating and modifying them.

### About policies and policy profiles

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

The status of the policy

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

Policies function according to the following rules:

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

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

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

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





Policy profiles function according to the following rules:

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

## About lock and locked settings

Each policy setting has a lock button icon (🔒). The table below shows lock button statuses:

Lock button statuses

| Status                                                                                                                                                                        | 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 <i>unlocked</i> .                                        |
|  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 <i>locked</i> . |

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:

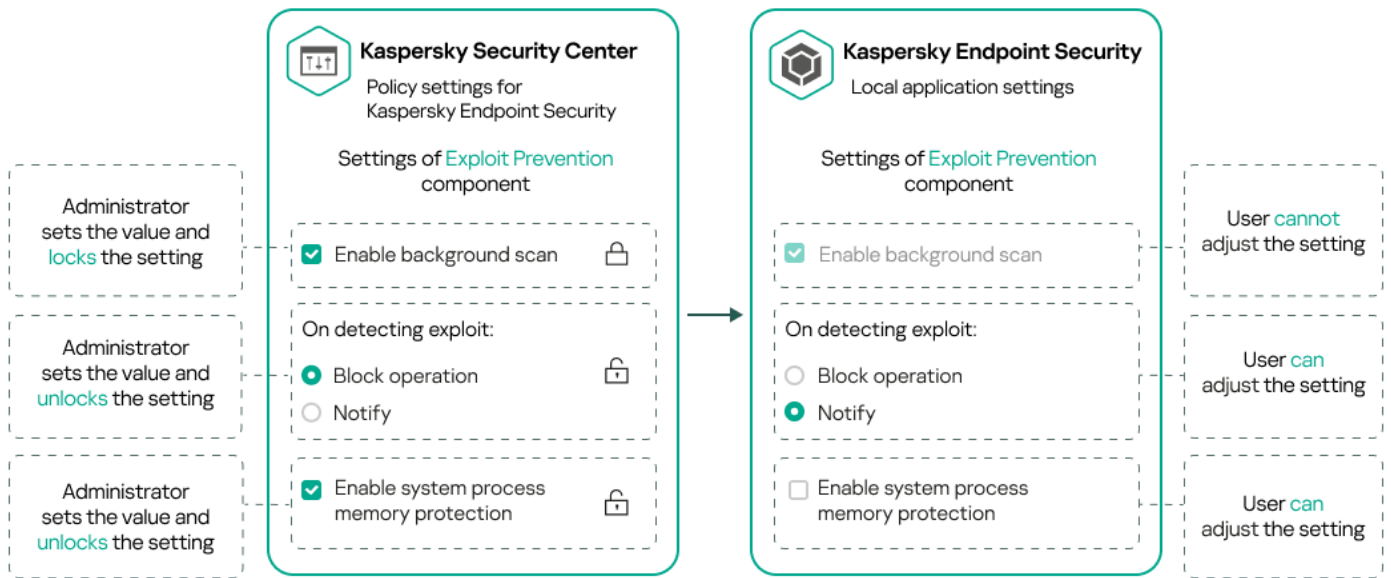
- Locking settings for an administration subgroup policy
- Locking settings of a Kaspersky application on a managed device

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

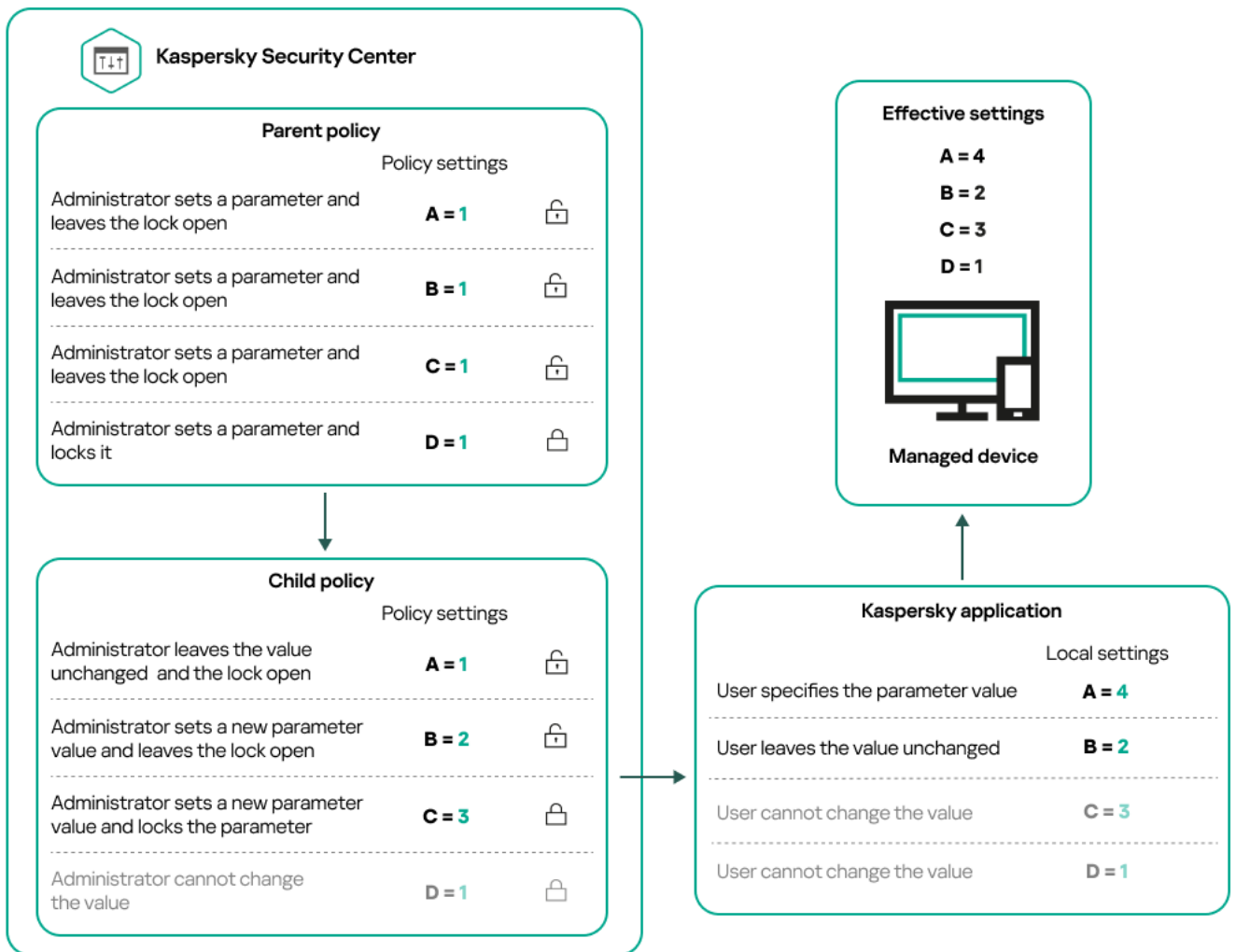
If different devices need different settings, you can organize devices into administration groups.

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).



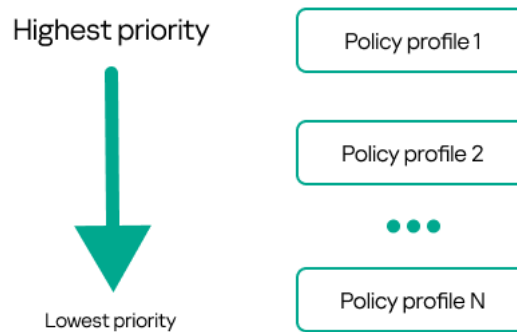
Hierarchy of policies

## Policy profiles in a hierarchy of policies

Policy profiles have the following priority assignment conditions:

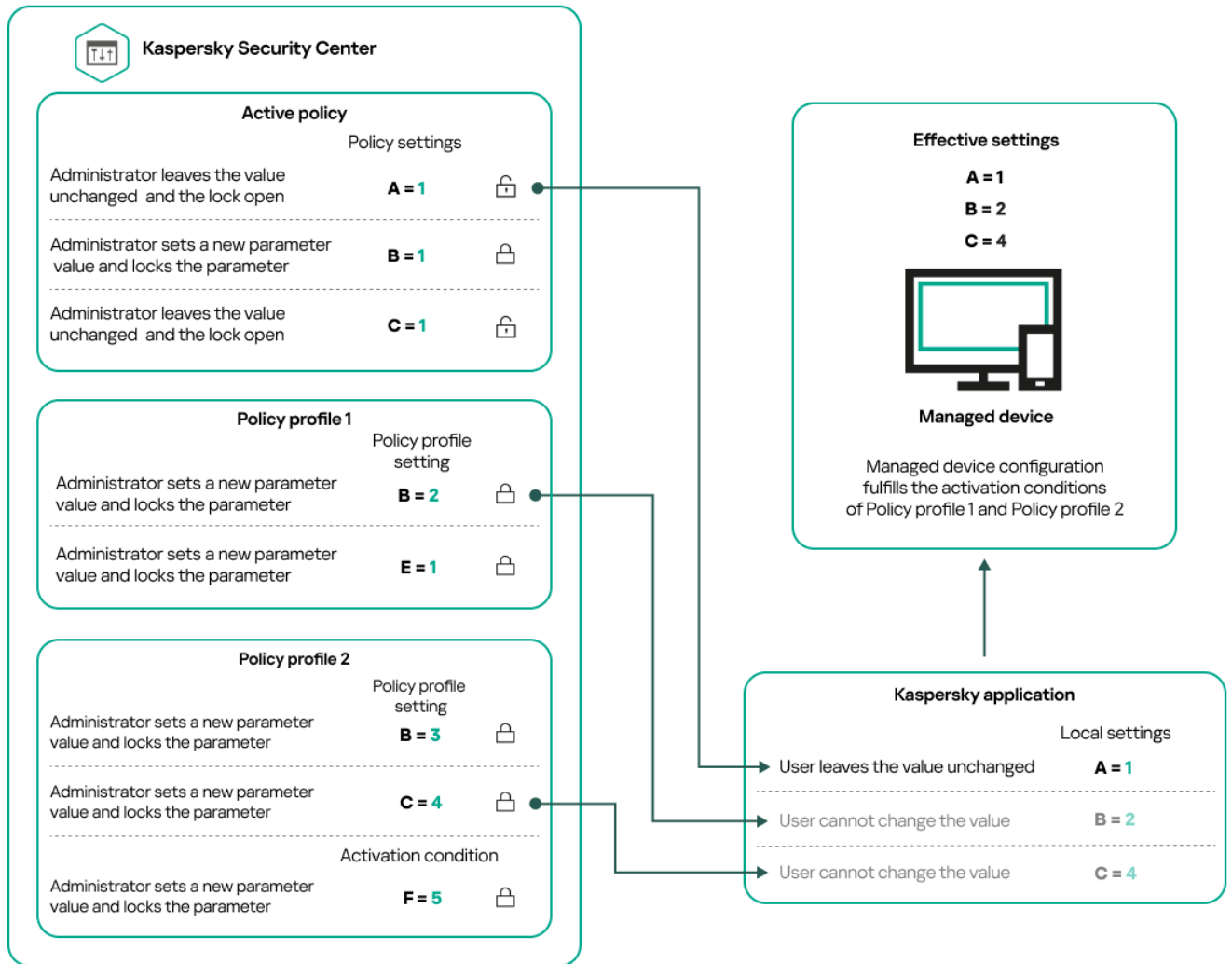
- A profile's position in a policy profile list indicates its priority. You can change a policy profile priority. The highest position in a list indicates the highest priority (see the figure below).

### List of policy profiles



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).

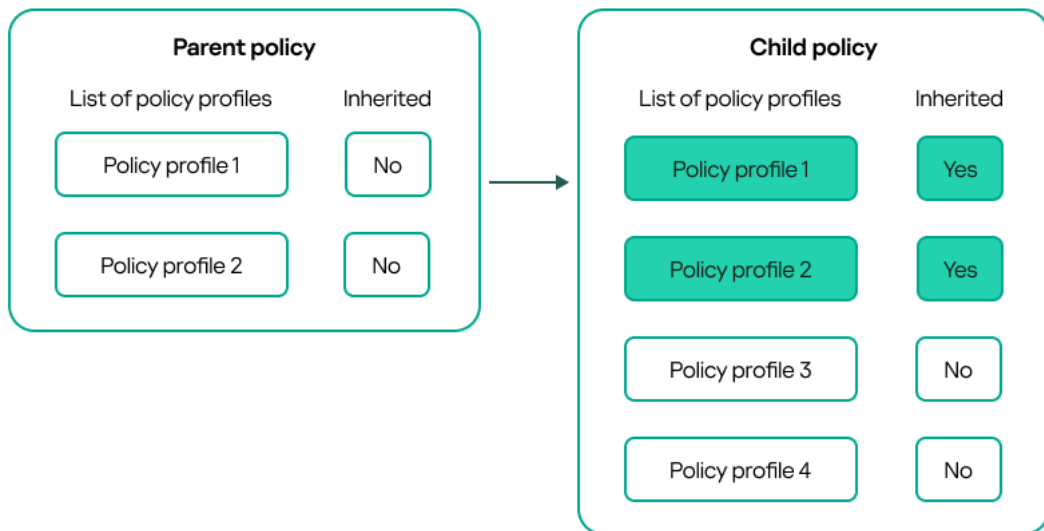


Managed device configuration fulfills activation conditions of several policy profiles

## 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).

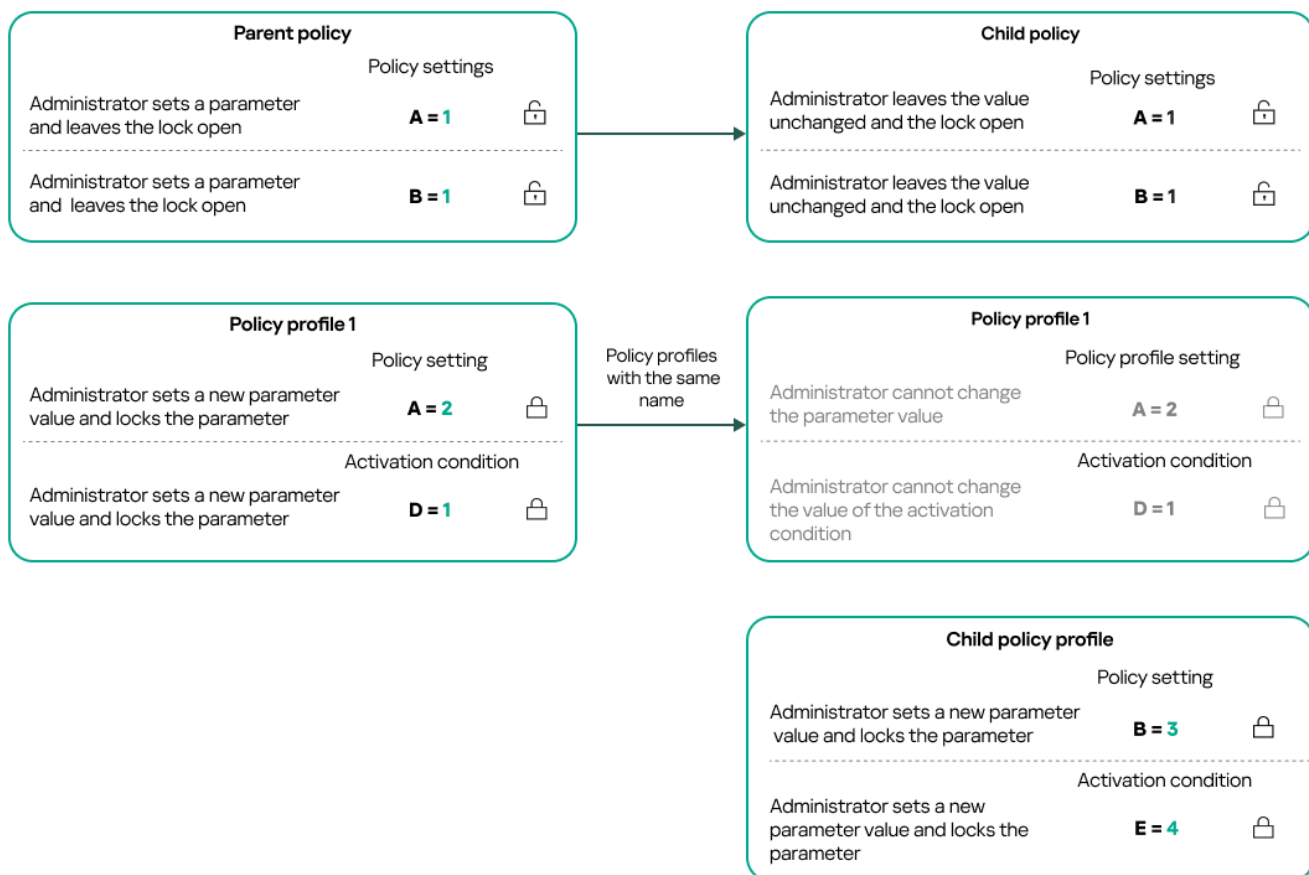


Inheritance of policy profiles

## 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 **Assets (Devices)** → **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 policy

You can create policies; you can also modify and delete existing policies.

*To create a policy:*

1. In the main menu, go to **Assets (Devices)** → **Policies & profiles**.
2. Click **Add**.  
The **Select application** window opens.
3. Select the application for which you want to create a policy.
4. Click **Next**.

The new policy settings window opens with the **General** tab selected.

5. If you want, change the default name, default status, and default inheritance settings of the policy.

6. 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.

7. On the **Application settings** tab, in the left pane select the category that you want and in the results' pane on the right, edit the settings of the policy. You can edit policy settings in each category (section).

The set of settings depends on the application for which you create a policy. For details, refer to the following:

- [Administration Server configuration](#)
- [Network Agent policy settings](#)
- [Kaspersky Endpoint Security for Linux Help](#) <sup>2</sup>
- [Kaspersky Endpoint Security for Windows Help](#) <sup>2</sup>

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.

8. Click **Save** to save the policy.

The policy will appear in the list of policies.

## 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](#) <sup>2</sup>

If this option is selected, the policy becomes active.  
By default, this option is selected.

- [Out-of-office](#) <sup>2</sup>

If this option is selected, the policy becomes active when the device leaves the corporate network.

- [Inactive](#) <sup>2</sup>

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](#) <sup>?</sup>

If this option is enabled, the policy setting values are inherited from the upper-level group policy and, therefore, are locked.

By default, this option is enabled.

- [Force inheritance of settings in child policies](#) <sup>?</sup>

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 term on the Administration Server (in days). Clicking an event type lets you specify the following settings:

- **Event registration**

You can specify how many days to store the event and select where to store the event:

- **Export to SIEM system using Syslog**
- **Store in the OS event log on device**
- **Store in the OS event log on Administration Server**

- **Event notifications**

You can select if you want to be notified about the event in one of the following ways:

- **Notify by email**
- **Notify by SMS**

- **Notify by running an executable file or script**
- **Notify by SNMP**

By default, the notification settings specified on the Administration Server properties tab (such as recipient address) are used. If you want, you can change these settings in the **Email**, **SMS**, and **Executable file to be run** tabs.

## Revision history

The **Revision history** tab allows you to view the list of the policy revisions and [roll back changes](#) made to the policy, if necessary.

## Modifying a policy

*To modify a policy:*

1. In the main menu, go to **Assets (Devices)** → **Policies & profiles**.
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:
  - [Administration Server configuration](#)
  - [Network Agent policy settings](#)
  - [Kaspersky Endpoint Security for Linux Help](#) <sup>☞</sup>
  - [Kaspersky Endpoint Security for Windows Help](#) <sup>☞</sup>

For details about settings of other security applications, refer to the documentation for that application.

4. Click **Save**.

The changes made to the policy will be saved in the policy properties, and will appear in the **Revision history** section.

## 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 **Assets (Devices) → Policies & profiles**.
2. Select the check box next to the policy (or policies) that you want to copy.
3. Click the **Copy** 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 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.

*To move a policy to another administration group:*

1. In the main menu, go to **Assets (Devices) → Policies & profiles**.

2. Select the check box next to the policy (or policies) that you want to move.

3. Click the **Move** button.

On the right side of the screen, the tree of the administration groups appears.

4. In the tree, select the target group, that is, the group to which you want to move the policy (or policies).

5. Click the **Move** button at the bottom of the screen.

6. Click **OK** to confirm the operation.

If a policy is not inherited from the source group, it is moved to the target group with all its profiles. The status of the policy in the target group is **Inactive**. You can change the status to **Active** at any time.

If a policy is inherited from the source group, it remains in the source group. It is copied to the target group with all its profiles. The status of the policy in the target group is **Inactive**. You can change the status to **Active** at any time.

If a policy with the name identical to that of the newly moved policy already exists in the target group, the name of the newly moved policy is expanded with the (<next sequence number>) index, for example: (1).

## Exporting a policy

Kaspersky Security Center Linux allows you to save a policy, its settings, and the policy profiles to a KLP file. You can use this KLP file to [import the saved policy](#), both to Kaspersky Security Center Windows and Kaspersky Security Center Linux.

*To export a policy:*

1. In the main menu, go to **Assets (Devices) → Policies & profiles**.

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 Security Center Linux allows you to import a policy from a KLP file. The KLP file contains the [exported policy](#), its settings, and the policy profiles.

*To import a policy:*

1. In the main menu, go to **Assets (Devices) → Policies & profiles**.

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)**.

## Forced synchronization

Although Kaspersky Security Center Linux automatically synchronizes the status, settings, tasks, and policies for managed devices, in some cases the administrator must know for certain, at a given moment, whether synchronization has already been performed for a specified device.

### Synchronizing a single device

*To force synchronization between the Administration Server and a managed device:*

1. In the main menu, go to **Assets (Devices) → Managed devices**.
2. Click the name of the device that you want to synchronize with the Administration Server.  
A property window opens with the **General** section selected.
3. Click the **Force synchronization** button.

The application synchronizes the selected device with the Administration Server.

### Synchronizing multiple devices

*To force synchronization between the Administration Server and multiple managed devices:*

1. Open the device list of an administration group or a device selection:

- In the main menu, go to **Assets (Devices)** → **Managed devices**, click the path link in the **Current path** field above the list of managed devices, then select the administration group that contains devices to synchronize.
- [Run a device selection](#) to view the device list.

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, the administrator can check whether the changed policy has been delivered to a specific managed device. A policy can be delivered during a regular synchronization or a forced synchronization.

*To view the date and time that an application policy was delivered to a managed device:*

1. In the main menu, go to **Assets (Devices)** → **Managed devices**.

2. Click the name of the device that you want to synchronize with the Administration Server.

A property window opens with the **General** section selected.

3. Click the **Applications** tab.

4. Select the application for which you want to view the policy synchronization date.

The application policy window opens with the **General** section selected and the policy delivery date and time displayed.

## Viewing the policy distribution status chart

In Kaspersky Security Center Linux, you can view the status of policy application on each device in a policy distribution status chart.

*To view the policy distribution status on each device:*

1. In the main menu, go to **Assets (Devices)** → **Policies & profiles**.

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, select the **Distribution** link.

The **<Policy name> distribution results** window opens.

4. In the **<Policy name> distribution results** window that opens, the **Status description** of the policy is displayed.

You can change number of results displayed in the list with policy distribution. The maximum number of devices is 100000.

*To change the number of devices displayed in the list with policy distribution results:*

1. In the main menu, go to your account settings, and then select **Interface options**.
2. In the **Limit of devices displayed in policy distribution results**, enter the number of devices (up to 100000).  
By default, the number is 5000.
3. Click **Save**.  
The settings are saved and applied.

## 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 **Assets (Devices) → Policies & profiles**.
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, and deleting a policy profile.

## Viewing the profiles of a policy

*To view profiles of a policy:*

1. In the main menu, go to **Assets (Devices) → Policies & profiles**.
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 a 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 the 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.

## 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 a 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 **Copy**.

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 **Copy**.

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).

Later, you can change the settings of the profile, including its name and its priority; the original policy profile will not be changed in this case.

## Creating a policy profile activation rule

*To create a policy profile activation rule:*

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 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.

- [Rule for Administration Server connection is active on this device](#)

Choose the condition of policy profile activation (whether the rule is executed or not) and select the rule name.

The rule defines the network location of the device for connection to the Administration Server, whose conditions must be met (or must not be met) for activation of the policy profile.

A network location description of devices for connection to an Administration Server can be created or configured in a Network Agent switching rule.

- **Rules for specific device owner**

For this option, specify at the next step:

- [Device owner](#)

Enable this option to configure and enable the rule for profile activation on the device according to its owner. In the drop-down list under the check box, you can select a criterion for the profile activation:

- The device belongs to the specified owner ("=" sign).
- The device does not belong to the specified owner ("#" sign).

If this option is enabled, the profile is activated on the device in accordance with the criterion configured. You can specify the device owner when the option is enabled. If this option is disabled, the profile activation criterion is not applied. By default, this option is disabled.

- [Device owner is included in an internal security\\_group](#)

Enable this option to configure and enable the rule of profile activation on the device by the owner's membership in an internal security group of Kaspersky Security Center Linux. In the drop-down list under the check box, you can select a criterion for the profile activation:

- The device owner is a member of the specified security group ("=" sign).
- The device owner is not a member of the specified security group ("#" sign).

If this option is enabled, the profile is activated on the device in accordance with the criterion configured. You can specify a security group of Kaspersky Security Center Linux. If this option is disabled, the profile activation criterion is not applied. By default, this option is disabled.

- [Rules for hardware specifications](#)

Select this check box to set up rules for policy profile activation on the device depending on the memory volume and the number of logical processors.

For this option, specify at the next step:

- [RAM size, in MB](#) 

Enable this option to configure and enable the rule of profile activation on the device by the RAM volume available on that device. In the drop-down list under the check box, you can select a criterion for the profile activation:

- The device RAM size is less than the specified value (" $<$ " sign).
- The device RAM size is greater than the specified value (" $>$ " sign).

If this option is enabled, the profile is activated on the device in accordance with the criterion configured. You can specify the RAM volume on the device. If this option is disabled, the profile activation criterion is not applied. By default, this option is disabled.

- [Number of logical processors](#) 

Enable this option to configure and enable the rule of profile activation on the device by the number of logical processors on that device. In the drop-down list under the check box, you can select a criterion for the profile activation:

- The number of logical processors on the device is less than or equal to the specified value (" $<=$ " sign).
- The number of logical processors on the device is greater than or equal to the specified value (" $>=$ " sign).

If this option is enabled, the profile is activated on the device in accordance with the criterion configured. You can specify the number of logical processors on the device. If this option is disabled, the profile activation criterion is not applied. By default, this option is disabled.

- **Rules for role assignment**

For this option, specify at the next step:

- [Activate policy profile by specific role of device owner](#) 

Select this option to configure and enable the rule of profile activation on the device depending on the owner's role. Add the role manually from the list of existing roles.

If this option is enabled, the profile is activated on the device in accordance with the criterion configured.

- [Rules for tag usage](#) 

Select this check box to set up rules for policy profile activation on the device depending on the tags assigned to the device. You can activate the policy profile to the devices that either have the selected tags or do not have them.

For this option, specify at the next step:

- [Tag list](#) 

In the list of tags, specify the rule for device inclusion in the policy profile by selecting the check boxes next to the relevant tags.

You can add new tags to the list by entering them in the field over the list and clicking the **Add** button.

The policy profile includes devices with descriptions containing all the selected tags. If check boxes are cleared, the criterion is not applied. By default, these check boxes are cleared.

- [Apply to devices without the specified tags](#) 

Enable this option if you have to invert your selection of tags.

If this option is enabled, the policy profile includes devices with descriptions that contain none of the selected tags. If this option is disabled, the criterion is not applied.

By default, this option is disabled.

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 a 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.

## Network Agent policy settings

To configure the Network Agent policy:

1. In the main menu, go to **Assets (Devices) → Policies & profiles**.
2. Click the name of the Network Agent policy.

The properties window of the Network Agent policy opens. The properties window contains the tabs and settings described below.

Consider that for Linux and Windows-based devices, [various settings](#) are available.

## General

On this tab, you can modify the policy name, policy status and specify the inheritance of policy settings:

- In the **Policy status** block, you can select one of the following policy modes:

- [Active policy](#) <sup>?</sup>

If this option is selected, the policy becomes active.

By default, this option is selected.

- [Inactive policy](#) <sup>?</sup>

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](#) <sup>?</sup>

If this option is enabled, the policy setting values are inherited from the upper-level group policy and, therefore, are locked.

By default, this option is enabled.

- [Force inheritance of settings in child policies](#) <sup>?</sup>

If this option is enabled, after policy changes are applied, the following actions will be performed:

- The values of the policy settings will be propagated to the policies of administration subgroups, that is, to the child policies.
- In the **Settings inheritance** block of the **General** section in the properties window of each child policy, the **Inherit settings from parent policy** option will be automatically enabled.

If this option is enabled, the child policies settings are locked.

By default, this option is disabled.

## Event configuration

On this tab, you can configure event logging and event notification. Events are distributed according to importance level in the following sections:

- **Functional failure**
- **Warning**
- **Info**

In each section, the list shows the types of events and the default event storage period on the Administration Server (in days). After you click the event type, you can specify the settings of event logging and notifications about events selected in the list. By default, common notification settings specified for the entire Administration Server are used for all event types. However, you can change specific settings for the required event types.

For example, in the **Warning** section, you can configure the **Security issue has occurred** event type. Such events may happen, for instance, when the [free disk space of a distribution point](#) is less than 2 GB (at least 4 GB are required to install applications and download updates remotely). To configure the **Security issue has occurred** event, click it and specify where to store the occurred events and how to notify about them.

If Network Agent detected a security issue, you can manage this issue by using the [settings of a managed device](#).

## Application settings

### Settings

In the **Settings** section, you can configure the Network Agent policy:

- [Distribute files through distribution points only](#) 

If this option is enabled, Network Agents on managed devices retrieve updates from distribution points only.

If this option is disabled, Network Agents on managed devices [retrieve updates from distribution points or from Administration Server](#).

Note that the security applications on managed devices retrieve updates from the source set in the update task for each security application. If you enable the **Distribute files through distribution points only** option, make sure that Kaspersky Security Center Linux is set as an update source in the update tasks.

By default, this option is disabled.

- [Maximum size of event queue, in MB](#) 

In this field you can specify the maximum space on the drive that an event queue can occupy.

The default value is 2 megabytes (MB).

- [Application is allowed to retrieve policy's extended data on device](#) 

Network Agent installed on a managed device transfers information about the applied security application policy to the security application (for example, Kaspersky Endpoint Security for Linux). You can view the transferred information in the security application interface.

Network Agent transfers the following information:

- Time of the policy delivery to the managed device
- Name of the active or out-of-office policy at the moment of the policy delivery to the managed device
- 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

You can use the information to ensure the correct policy is applied to the device and for troubleshooting purposes. By default, this option is disabled.

- [Protect the Network Agent service against unauthorized removal or termination, and prevent changes to the settings](#) 

When this option is enabled, after Network Agent is installed on a managed device, the component cannot be removed or reconfigured without required privileges. The Network Agent service cannot be stopped. This option has no effect on domain controllers.

Enable this option to protect Network Agent on workstations operated with local administrator rights.

By default, this option is disabled.

- [Use uninstallation password](#) 

If this option is enabled, by clicking the **Modify** button you can specify the password for the klmover utility and Network Agent remote uninstallation.

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](#) 

If this option is enabled, information about applications installed on client devices is sent to the Administration Server.

By default, this option is enabled.

- [Hardware registry details](#) 

Network Agent installed on a device sends information about the device hardware to the Administration Server. You can view the hardware details in the device properties.

Ensure that the lshw utility is installed on Linux devices from which you want to fetch hardware details. Hardware details fetched from virtual machines may be incomplete depending on the hypervisor used.

## Connectivity

The **Connectivity** section includes three subsections:

- **Network**
- **Connection profiles**
- **Connection schedule**

In the **Network** subsection, you can configure the connection to Administration Server, enable the use of a UDP port, and specify the UDP port number.

- In the **Connect to Administration Server** settings group, you can configure connection to the Administration Server and specify the time interval for synchronization between client devices and the Administration Server:

- [Synchronization interval \(min\)](#) 

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

If the synchronization interval is set to less than 15 minutes, synchronization is performed every 15 minutes. If synchronization interval is set to 15 minutes or more, synchronization is performed at the specified synchronization interval.

- [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, a UDP port, necessary for the work of Network Agent, is added to the Microsoft Windows Firewall exclusion list.

By default, this option is enabled.

- [Use SSL connection](#) 



If this option is enabled, connection to the Administration Server is established through a secure port via SSL.

By default, this option is enabled.

- [Use connection gateway on distribution point \(if available\) under 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, this option is enabled.

- [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, this option is enabled. The default UDP port to connect to the KSN proxy server is 15111.

- [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.

In the **Connection profiles** subsection, you can specify the network location settings and enable out-of-office mode when Administration Server is not available. The settings in the **Connection profiles** section are available only on devices running Windows:

- [Network location settings](#)

Network location settings define the characteristics of the network to which the client device is connected and specify rules for Network Agent switching from one Administration Server connection profile to another when those network characteristics are altered.

- [Administration Server connection profiles](#)

Connection profiles are supported only for devices running Windows.

You can view and add profiles for Network Agent connection to the Administration Server. In this section, you can also create rules for switching Network Agent to different Administration Servers when the following events occur:

- When the client device connects to a different local network
- When the device loses connection with the local network of the organization
- When the connection gateway address is changed or the DNS server address is modified

- [Enable out-of-office mode when Administration Server is not available](#)

If this option is enabled, in case of connection through this profile, applications installed on the client device use policy profiles for devices in out-of-office mode, as well as out-of-office policies. If no out-of-office policy has been defined for the application, the active policy will be used.

If this option is disabled, applications will use active policies.

By default, this option is disabled.

In the **Connection schedule** subsection, you can specify the time intervals during which Network Agent sends data to the Administration Server:

- [Connect when necessary](#) <sup>?</sup>

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](#) <sup>?</sup>

If this option is selected, Network Agent connects to the Administration Server at a specified time. You can add several connection time periods.

## Network polling by distribution points

In the **Network polling by distribution points** section, you can configure automatic polling of the network. You can use the following options to enable the polling and set its frequency:

- [Zeroconf](#) <sup>?</sup>

If this option is enabled, the distribution point automatically polls the network with IPv6 devices by using [zero-configuration networking](#) (also referred to as *Zeroconf*). In this case, the enabled IP range polling is ignored, because the distribution point polls the whole network.

To start to use Zeroconf, the following conditions must be fulfilled:

- The distribution point must run Linux.
- You must install the avahi-browse utility on the distribution point.

If this option is disabled, the distribution point does not poll networks with IPv6 devices.

By default, this option is disabled.

- [IP ranges](#) <sup>?</sup>

If the option is enabled, the distribution point automatically polls IP ranges according to the schedule that you configured by clicking the **Set polling schedule** button.

If this option is disabled, the distribution point does not poll IP ranges.

The frequency of IP range polling for Network Agent versions prior to 10.2 can be configured in the **Poll interval (min)** field. The field is available if the option is enabled.

By default, this option is disabled.

- [Domain controllers](#) <sup>?</sup>

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**
- **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.

By default, this check box is cleared.

- **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 Kaspersky Security Network (KSN) requests from the managed devices:

- **[Enable KSN Proxy on the distribution point side](#)** 

The KSN proxy service is run on the device that is used as a distribution point. Use this feature to redistribute and optimize traffic on the network.

The distribution point sends the KSN statistics, which are listed in the Kaspersky Security Network statement, to Kaspersky.

By default, this option is disabled. Enabling this option takes effect only if the **Use Administration Server as a proxy server** and **I agree to use Kaspersky Security Network** options are enabled in the Administration Server properties window.

You can assign a node of an active-passive cluster to a distribution point and enable KSN proxy server on this node.

- [Forward KSN requests to Administration Server](#) 

The distribution point forwards KSN requests from the managed devices to the Administration Server.

By default, this option is enabled.

- [Access KSN Cloud/KPSN directly over the internet](#) 

The distribution point forwards KSN requests from managed devices to the KSN Cloud or KPSN. The KSN requests generated on the distribution point itself are also sent directly to the KSN Cloud or KPSN.

- [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 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, this option is enabled. The default UDP port to connect to the KSN proxy server is 15111.

## Updates (distribution points)

In the **Updates (distribution points)** section, you can enable the [downloading diff files feature](#), so distribution points take updates in the form of diff files from Kaspersky update servers.

## 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. The settings in the **Restart management** section are available only on devices running Windows:

- [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, this 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, this 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.

## Usage of Network Agent for Windows, Linux, and macOS: comparison

The Network Agent usage varies depending on the operating system of the device. The Network Agent policy and [installation package](#) settings also differ depending on the operating system. The table below compares Network Agent features and usage scenarios available for Windows, Linux, and macOS operating systems.

Network Agent feature comparison

| Network Agent feature                                                                                                                                | Windows | Linux                                                | macOS                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------------------------------------------------------|------------------------------------------------------|
| <b>Installation</b>                                                                                                                                  |         |                                                      |                                                      |
| <a href="#">Installing by cloning an image of the administrator's hard drive with the operating system and Network Agent using third-party tools</a> | ✓       | ✓                                                    | —                                                    |
| Installing with third-party tools for remote installation of applications                                                                            | ✓       | ✓                                                    | ✓                                                    |
| Installing manually, by running application installers on devices                                                                                    | ✓       | ✓                                                    | ✓                                                    |
| <a href="#">Installing Network Agent in silent mode</a>                                                                                              | ✓       | ✓                                                    | ✓                                                    |
| Manually connecting a client device to the Administration Server. klmover utility                                                                    | ✓       | ✓                                                    | ✓                                                    |
| Automatic installing of updates and patches for Kaspersky Security Center components                                                                 | ✓       | —                                                    | —                                                    |
| Automatic distributing of a key                                                                                                                      | ✓       | ✓                                                    | ✓                                                    |
| Forced synchronization                                                                                                                               | ✓       | ✓                                                    | ✓                                                    |
| <b>Distribution point</b>                                                                                                                            |         |                                                      |                                                      |
| <a href="#">Using as distribution point</a>                                                                                                          | ✓       | ✓                                                    | ✓                                                    |
| <a href="#">Automatic assignment of distribution points</a>                                                                                          | ✓       | ✓<br>Without using Network Location Awareness (NLA). | ✓<br>Without using Network Location Awareness (NLA). |
| Offline model of update download                                                                                                                     | ✓       | ✓                                                    | ✓                                                    |
| Network polling                                                                                                                                      | ✓       | ✓                                                    | —                                                    |

|                                                                                                                                     |                                                                                                           |                                                                                                                                                                                              |                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                     | <ul style="list-style-type: none"> <li>• IP range polling</li> <li>• Domain controller polling</li> </ul> | <ul style="list-style-type: none"> <li>• IP range polling</li> <li>• Zeroconf polling</li> <li>• Domain controller polling (Microsoft Active Directory, Samba 4 Active Directory)</li> </ul> |                                                                                                                                                                                                                                                             |
| 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 | ✓                                                                                                         | ✓                                                                                                                                                                                            | —<br>(If one or more devices running Linux or macOS are within the scope of the Download updates to the repositories of distribution points task, the task completes with the Failed status, even if it has successfully completed on all Windows devices.) |
| Push installation of applications                                                                                                   | ✓                                                                                                         | 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.                                                                                                                                          |
| Using as a push server                                                                                                              | ✓                                                                                                         | ✓                                                                                                                                                                                            | —                                                                                                                                                                                                                                                           |
| <b>Handling third-party applications</b>                                                                                            |                                                                                                           |                                                                                                                                                                                              |                                                                                                                                                                                                                                                             |
| <a href="#">Remote installing of applications on devices</a>                                                                        | ✓                                                                                                         | ✓                                                                                                                                                                                            | ✓                                                                                                                                                                                                                                                           |
| Configuring operating system updates in a Network Agent policy                                                                      | ✓                                                                                                         | —                                                                                                                                                                                            | —                                                                                                                                                                                                                                                           |
| Viewing information about software vulnerabilities                                                                                  | ✓                                                                                                         | —                                                                                                                                                                                            | —                                                                                                                                                                                                                                                           |
| Scanning applications for vulnerabilities                                                                                           | ✓                                                                                                         | —                                                                                                                                                                                            | —                                                                                                                                                                                                                                                           |
| Software updates                                                                                                                    | ✓                                                                                                         | —                                                                                                                                                                                            | —                                                                                                                                                                                                                                                           |
| Inventory of software installed on devices                                                                                          | ✓                                                                                                         | ✓                                                                                                                                                                                            | —                                                                                                                                                                                                                                                           |
| <b>Virtual machines</b>                                                                                                             |                                                                                                           |                                                                                                                                                                                              |                                                                                                                                                                                                                                                             |
| <a href="#">Installing Network Agent on a virtual machine</a>                                                                       | ✓                                                                                                         | ✓                                                                                                                                                                                            | ✓                                                                                                                                                                                                                                                           |
|                                                                                                                                     |                                                                                                           |                                                                                                                                                                                              |                                                                                                                                                                                                                                                             |

|                                                                                                       |   |   |                                                           |
|-------------------------------------------------------------------------------------------------------|---|---|-----------------------------------------------------------|
| <a href="#">Optimization settings for virtual desktop infrastructure (VDI).</a>                       | ✓ | ✓ | ✓                                                         |
| <a href="#">Support of dynamic virtual machines</a>                                                   | ✓ | ✓ | ✓                                                         |
| <b>Other</b>                                                                                          |   |   |                                                           |
| Auditing actions on a remote client device by using Windows Desktop Sharing                           | ✓ | — | —                                                         |
| Monitoring the anti-virus protection status                                                           | ✓ | ✓ | ✓                                                         |
| Managing device restarts                                                                              | ✓ | — | —                                                         |
| <a href="#">Support of file system rollback</a>                                                       | ✓ | ✓ | ✓                                                         |
| Using a Network Agent as connection gateway                                                           | ✓ | ✓ | ✓                                                         |
| Connection Manager                                                                                    | ✓ | ✓ | ✓                                                         |
| Network Agent switching from one Administration Server to another (automatically by network location) | ✓ | — | ✓                                                         |
| Checking the connection between a client device and the Administration Server. klnagchk utility       | ✓ | ✓ | ✓                                                         |
| Remotely connecting to the desktop of a client device                                                 | ✓ | — | ✓<br>By using the Virtual Network Computing (VNC) system. |
| Downloading a stand-alone installation package through the Migration wizard                           | ✓ | ✓ | ✓                                                         |

## Comparison of Network Agent settings by operating systems

The table below shows which Network Agent settings are available depending on the operating system of the managed device where Network Agent was installed.

Network Agent settings: comparison by operating systems

| Settings section           | Windows | Linux                                     | macOS |
|----------------------------|---------|-------------------------------------------|-------|
| <b>General</b>             | ✓       | ✓                                         | ✓     |
| <b>Event configuration</b> | ✓       | ✓                                         | ✓     |
| <b>Settings</b>            | ✓       | ✓<br>The following options are available: | ✓     |



|                                          |                                                                                                                                                                                                  |                                                                                                                                                                                                                                    |   |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
|                                          |                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• Distribute files through distribution points only</li> <li>• Maximum size of event queue, in MB</li> <li>• Application is allowed to retrieve policy's extended data on device</li> </ul> |   |
| Repositories                             | ✓                                                                                                                                                                                                | <p style="text-align: center;">✓</p> The following options are available: <ul style="list-style-type: none"> <li>• Details of installed applications</li> <li>• Hardware registry details</li> </ul>                               | — |
| Connectivity → Network                   | ✓                                                                                                                                                                                                | <p style="text-align: center;">✓</p> Except the <b>Open Network Agent ports in Microsoft Windows Firewall</b> option.                                                                                                              | ✓ |
| Connectivity → Connection profiles       | ✓                                                                                                                                                                                                | —                                                                                                                                                                                                                                  | ✓ |
| Connectivity → Connection schedule       | ✓                                                                                                                                                                                                | ✓                                                                                                                                                                                                                                  | ✓ |
| Network polling by distribution points   | <p style="text-align: center;">✓</p> The following options are available: <ul style="list-style-type: none"> <li>• Windows network</li> <li>• IP ranges</li> <li>• Domain controllers</li> </ul> | <p style="text-align: center;">✓</p> The following options are available: <ul style="list-style-type: none"> <li>• Zeroconf</li> <li>• IP ranges</li> <li>• Domain controllers</li> </ul>                                          | — |
| Network settings for distribution points | ✓                                                                                                                                                                                                | ✓                                                                                                                                                                                                                                  | ✓ |
| KSN Proxy (distribution points)          | ✓                                                                                                                                                                                                | ✓                                                                                                                                                                                                                                  | — |
| Updates (distribution points)            | ✓                                                                                                                                                                                                | ✓                                                                                                                                                                                                                                  | — |
| Revision history                         | ✓                                                                                                                                                                                                | ✓                                                                                                                                                                                                                                  | ✓ |

## Manual setup of the Kaspersky Endpoint Security policy

This section provides recommendations on how to configure the Kaspersky Endpoint Security policy. You can perform setup in the policy properties window. When you edit a setting, click the lock icon to the right of the relevant group of settings to apply the specified values to a workstation.

## Configuring Kaspersky Security Network

Kaspersky Security Network (KSN) is the infrastructure of cloud services that contains information about the reputation of files, web resources, and software. Kaspersky Security Network enables Kaspersky Endpoint Security for Windows to respond faster to different kinds of threats, enhances the performance of the protection components, and decreases the likelihood of false positives. For more information about Kaspersky Security Network, see the [Kaspersky Endpoint Security for Windows Help](#).

To specify recommended KSN settings:

1. In the main menu, go to **Assets (Devices) → Policies & profiles**.
2. Click the policy of Kaspersky Endpoint Security for Windows.  
The properties window of the selected policy opens.
3. In the policy properties, go to **Application settings → Advanced Threat Protection → Kaspersky Security Network**.
4. Make sure that the **Use KSN Proxy** option is enabled. Using this option helps to redistribute and optimize traffic on the network.

If you use [Managed Detection and Response](#), you must enable [KSN Proxy](#) option for the distribution point and [enable extended KSN mode](#).

5. [optional] Enable use of KSN servers if the KSN proxy service is not available. KSN servers may be located either on the side of Kaspersky (when KSN is used) or on the side of third parties (when KPSN is used).
6. Click **OK**.

The recommended KSN settings are specified.

## Checking the list of the networks protected by Firewall

Make sure that Kaspersky Endpoint Security for Windows Firewall protects all your networks. By default, Firewall protects networks with the following types of connection:

- **Public network.** Anti-virus applications, firewalls, or filters do not protect devices in such a network.
- **Local network.** Access to files and printers is restricted for devices in this network.
- **Trusted network.** Devices in such a network are protected from attacks and unauthorized access to files and data.

If you configured a custom network, make sure that Firewall protects it. For this purpose, check the list of the networks in the Kaspersky Endpoint Security for Windows policy properties. The list may not contain all the networks.

For more information about Firewall, see the [Kaspersky Endpoint Security for Windows Help](#).

*To check the list of networks:*

1. In the main menu, go to **Assets (Devices)** → **Policies & profiles**.
2. Click the policy of Kaspersky Endpoint Security for Windows.  
The properties window of the selected policy opens.
3. In the policy properties, go to **Application settings** → **Essential Threat Protection** → **Firewall**.
4. Under **Available networks**, click the **Network settings** link.  
The **Network connections** window opens. This window displays the list of networks.
5. If the list has a missing network, add it.

## Disabling the scan of network devices

When Kaspersky Endpoint Security for Windows scans network drives, this can place a significant load on them. It is more convenient to perform indirect scanning on file servers.

You can disable scanning of network drives in the Kaspersky Endpoint Security for Windows policy properties. For a description of these policy properties, see the [Kaspersky Endpoint Security for Windows Help](#).

*To disable scanning of network drives:*

1. In the main menu, go to **Assets (Devices)** → **Policies & profiles**.
2. Click the policy of Kaspersky Endpoint Security for Windows.  
The properties window of the selected policy opens.
3. In the policy properties, go to **Application settings** → **Essential Threat Protection** → **File Threat Protection**.
4. Under **Protection scope**, disable the **All network drives** option.
5. Click **OK**.

Scanning of network drives is disabled.

## Excluding software details from the Administration Server memory

We recommend that Administration Server does not save information about software modules that are started on the network devices. As a result, the Administration Server memory does not overrun.

You can disable saving this information in the Kaspersky Endpoint Security for Windows policy properties.

*To disable saving information about installed software modules:*

1. In the main menu, go to **Assets (Devices)** → **Policies & profiles**.
2. Click the policy of Kaspersky Endpoint Security for Windows.

The properties window of the selected policy opens.

3. In the policy properties, go to **Application settings** → **General Settings** → **Reports and Storage**.
4. Under **Data transfer to Administration Server**, disable the **About started applications** check box if it is still enabled in the top-level policy.

When this check box is selected, the Administration Server database saves information about all versions of all software modules on the networked devices. This information may require a significant amount of disk space in the Kaspersky Security Center Linux database (dozens of gigabytes).

The information about installed software modules is no longer saved to the Administration Server database.

## Configuring access to the Kaspersky Endpoint Security for Windows interface on workstations

If the Anti-Virus protection on the organization's network must be managed in centralized mode through Kaspersky Security Center Linux, specify the interface settings in the Kaspersky Endpoint Security for Windows policy properties, as described below. As a result, you will prevent unauthorized access to Kaspersky Endpoint Security for Windows on workstations and the changing of Kaspersky Endpoint Security for Windows settings.

For a description of these policy properties, see the [Kaspersky Endpoint Security for Windows Help](#).

*To specify recommended interface settings:*

1. In the main menu, go to **Assets (Devices)** → **Policies & profiles**.
2. Click the policy of Kaspersky Endpoint Security for Windows.  
The properties window of the selected policy opens.
3. In the policy properties, go to **Application settings** → **General Settings** → **Interface**.
4. Under **Interaction with user**, select the **No interface** option. This disables the display of the Kaspersky Endpoint Security for Windows user interface on workstations, so their users cannot change the settings of Kaspersky Endpoint Security for Windows.
5. Under **Password protection**, enable the toggle switch. This reduces the risk of unauthorized or unintended changes in the settings of Kaspersky Endpoint Security for Windows on workstations.

The recommended settings for the interface of Kaspersky Endpoint Security for Windows are specified.

## Saving important policy events in the Administration Server database

To avoid the Administration Server database overflow, we recommend that you save only important events to the database.

*To configure registration of important events in the Administration Server database:*

1. In the main menu, go to **Assets (Devices)** → **Policies & profiles**.

2. Click the policy of Kaspersky Endpoint Security for Windows.

The properties window of the selected policy opens.

3. In the policy properties, open the **Event configuration** tab.

4. In the **Critical** section, click **Add event** and select check boxes next to the following events only:

- *End User License Agreement violated*
- *Application autorun is disabled*
- *Activation error*
- *Active threat detected. Advanced Disinfection should be started*
- *Disinfection impossible*
- *Previously opened dangerous link detected*
- *Process terminated*
- *Network activity blocked*
- *Network attack detected*
- *Application startup prohibited*
- *Access denied (local bases)*
- *Access denied (KSN)*
- *Local update error*
- *Cannot start two tasks at the same time*
- *Error in interaction with Kaspersky Security Center*
- *Not all components were updated*
- *Error applying file encryption / decryption rules*
- *Error enabling portable mode*
- *Error disabling portable mode*
- *Could not load encryption module*
- *Policy cannot be applied*
- *Error changing application components*

5. Click **OK**.

6. In the **Functional failure** section, click **Add event** and select check box next to the event *Invalid task settings. Settings not applied*.

7. Click **OK**.

8. In the **Warning** section, click **Add event** and select check boxes next to the following events only:

- *Self-Defense is disabled*
- *Protection components are disabled*
- *Incorrect reserve key*
- *Legitimate software that can be used by intruders to damage your computer or personal data was detected (local bases)*
- *Legitimate software that can be used by intruders to damage your computer or personal data was detected (KSN)*
- *Object deleted*
- *Object disinfected*
- *User has opted out of the encryption policy*
- *File was restored from quarantine on the Kaspersky Anti Targeted Attack Platform server by the administrator*
- *File was quarantined on the Kaspersky Anti Targeted Attack Platform server by administrator*
- *Application startup blockage message to administrator*
- *Device access blockage message to administrator*
- *Web page access blockage message to administrator*

9. Click **OK**.

10. In the **Info** section, click **Add event** and select check boxes next to the following events only:

- *A backup copy of the object was created*
- *Application startup prohibited in test mode*

11. Click **OK**.

Registration of important events in the Administration Server database is configured.

## 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.

# 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.

## About KSN

Kaspersky Security Network (KSN) is an online service infrastructure that provides access to the online Knowledge Base of Kaspersky, which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the effectiveness of some protection components, and reduces the risk of false positives. KSN allows you to use Kaspersky reputation databases to retrieve information about applications installed on managed devices.

By participating in KSN, you agree to send to Kaspersky in automatic mode information about the operation of Kaspersky applications installed on client devices that are managed through Kaspersky Security Center Linux. Information is transferred in accordance with the current [KSN access settings](#).

Kaspersky Security Center Linux supports the following KSN infrastructure solutions:

- *Global KSN* is a solution that allows you to exchange information with Kaspersky Security Network. 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 Security Center Linux. Information is transferred in accordance with the current [KSN access settings](#). Kaspersky analysts additionally analyze received information and include it in the reputation and statistical databases of Kaspersky Security Network. Kaspersky Security Center Linux uses this solution by default.
- *Kaspersky Private Security Network (KPSN)* is a solution that allows users of devices with Kaspersky applications installed to obtain access to reputation databases of Kaspersky Security Network, and other statistical data, without sending data to KSN from their own computers. KPSN is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:
  - User devices are not connected to the internet.
  - Transmission of any data outside the country or outside the corporate LAN is prohibited by law or restricted by corporate security policies.

You can [set up access settings](#) of Kaspersky Private Security Network in the **KSN Proxy settings** section of the Administration Server properties window.

The application prompts you to join KSN while running the [quick start wizard](#). You can start or stop using KSN at any moment when [using the application](#).

You use KSN in accordance with the KSN Statement that you read and accept when you enable KSN. If the KSN Statement is updated, it is displayed to you when you 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 Security Center Linux 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 configure the KSN proxy server in the **KSN Proxy settings** section of the [Administration Server properties window](#).

## Setting up access to KSN

You can set up access to Kaspersky Security Network (KSN) on the Administration Server and on a distribution point.

*To set up Administration Server access to KSN:*

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 **KSN Proxy settings** section.

3. Switch the toggle button to the **Enable KSN Proxy on Administration Server Enabled** position.

Data is sent from client devices to KSN in accordance with the Kaspersky Endpoint Security policy, which is active on those client devices. If this check box is cleared, no data will be sent to KSN from the Administration Server and client devices through Kaspersky Security Center Linux. However, client devices can send data to KSN directly (bypassing Kaspersky Security Center Linux), in accordance with their respective settings. The Kaspersky Endpoint Security policy, which is active on client devices, determines which data will be sent directly (bypassing Kaspersky Security Center Linux) from those devices to KSN.

4. Switch the toggle button to the **Use Kaspersky Security Network Enabled** position.

If this option is enabled, client devices send patch installation results to Kaspersky. When enabling this option, make sure to read and accept the terms of the KSN Statement.

If you are using [KPSN@](#), switch the toggle button to the **Use Kaspersky Private Security Network Enabled** position and click the **Select file with KSN Proxy settings** button to download the settings of KPSN (files with the extensions pkcs7 and pem). After the settings are downloaded, the interface displays the provider's name and contacts, as well as the creation date of the file with the settings of KPSN.

When you switch the toggle button to the **Use Kaspersky Private Security Network Enabled** position, a message appears with details about KPSN.

The following Kaspersky applications support KPSN:

- Kaspersky Security Center Linux
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

If you enable KPSN in Kaspersky Security Center Linux, these applications receive information about supporting KPSN. In the settings window of the application, in the **Kaspersky Security Network** subsection of the **Advanced Threat Protection** section, the information about selected KSN provider is displayed — KSN or KPSN.



Kaspersky Security Center Linux does not send any statistical data to Kaspersky Security Network if KPSN is configured in the **KSN Proxy settings** section of the Administration Server properties window.

5. If you have the proxy server settings configured in the Administration Server properties, but your network architecture requires that you use KPSN directly, enable the **Ignore proxy server settings when connecting to KPSN** option. Otherwise, requests from the managed applications cannot reach KPSN.

6. Configure the Administration Server connection to the KSN proxy service:

- Under **Connection settings**, for the **TCP port**, specify the number of the TCP port that will be used for connecting to the KSN proxy server. The default port to connect to the KSN proxy server is 13111.
- If you want the Administration Server to connect to the KSN proxy server through a UDP port, enable the **Use UDP port** option and specify a port number for the **UDP port**. By default, this option is disabled, and TCP port is used. If this option is enabled, the default UDP port to connect to the KSN proxy server is 15111.

7. Switch the toggle button to the **Connect secondary Administration Servers to KSN through primary Administration Server Enabled** position.

If this option is enabled, secondary Administration Servers use the primary Administration Server as the KSN proxy server. If this option is disabled, secondary Administration Servers connect to KSN on their own. In this case, managed devices use secondary Administration Servers as KSN proxy servers.

Secondary Administration Servers use the primary Administration Server as a proxy server if in the right pane of the **KSN Proxy settings** section, in the properties of secondary Administration Servers the toggle button is switched to the **Enable KSN Proxy on Administration Server Enabled** position.

8. Click the **Save** button.

The KSN access settings will be saved.

You can also set up distribution point access to KSN, for example, if you want to reduce the load on the Administration Server. The distribution point that acts as a KSN proxy server sends KSN requests from managed devices to Kaspersky directly, without using the Administration Server.

*To set up distribution point access to Kaspersky Security Network (KSN):*

1. Make sure that the distribution point is [assigned manually](#).
2. In the main menu, click the settings icon (⚙️) next to the name of the required Administration Server.  
The Administration Server properties window opens.
3. On the **General** tab, select the **Distribution points** section.
4. Click the name of the distribution point to open its properties window.
5. In the distribution point properties window, in the **KSN Proxy** section, enable the **Enable KSN Proxy on the distribution point side** option, and then enable the **Access KSN Cloud/KPSN directly over the internet** option.
6. Click **OK**.

The distribution point will act as a KSN proxy server.

Please note that the distribution point does not support managed device authentication by using the NTLM protocol.

## Enabling and disabling KSN

*To enable KSN:*

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 **KSN Proxy settings** section.

3. Switch the toggle button to the **Enable KSN Proxy on Administration Server Enabled** position.  
The KSN proxy server is enabled.

4. Switch the toggle button to the **Use Kaspersky Security Network Enabled** position.  
KSN will be 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.

5. Click the **Save** button.

*To disable KSN:*

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 **KSN Proxy settings** section.

3. Switch the toggle button to the **Enable KSN Proxy on Administration Server Disabled** position to disable the KSN proxy service, or switch the toggle button to the **Use Kaspersky Security Network Disabled** position.

If one of these toggle buttons is disabled, client devices will send no patch installation results to Kaspersky.

If you are using KPSN, switch the toggle button to the **Use Kaspersky Private Security Network Disabled** position.

KSN will be disabled.

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 settings icon (⚙️) next to the name of the required Administration Server.

The Administration Server properties window opens.

2. On the **General** tab, select the **KSN Proxy 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 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 will continue using KSN in accordance with the version of the KSN Statement that you previously accepted.

After updating or upgrading Administration Server, the updated KSN Statement is displayed automatically. If you decline the updated KSN Statement, you can still view and accept it later.

*To view and then accept or decline an updated KSN Statement:*

1. Click the **View notifications** link in the upper-right corner of the main application window.  
The **Notifications** window opens.
2. Click the **View the updated KSN Statement** link.  
The **Kaspersky Security Network Statement update** window opens.
3. Read the KSN Statement, and then make your decision by clicking one of the following buttons:
  - **I accept the updated KSN Statement**
  - **Use KSN under the old Statement**

Depending on your choice, KSN keeps working in accordance with the terms of the current or updated KSN Statement. You can [view the text of the accepted KSN Statement](#) in the properties of Administration Server at any time.

## Checking whether the distribution point works as KSN proxy server

On a managed device assigned to work as a distribution point, you can enable Kaspersky Security Network (KSN) Proxy. A managed device works as the KSN proxy server when the ksnproxy service is running on the device. You can check, turn on, or turn off this service on the device locally.

You can assign a Windows-based or a Linux-based device as a distribution point. The method of distribution point checking depends on the operating system of this distribution point.

*To check whether the Linux-based distribution point works as KSN proxy server:*

1. On the distribution point device, 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.

*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.

## Managing tasks

This section describes tasks used by Kaspersky Security Center Linux.

## About tasks

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

Tasks for a specific application can be created using Kaspersky Security Center Web Console only if the management plug-in for that application is installed on Kaspersky Security Center Web Console Server.

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

The tasks that are performed on the Administration Server include the following:

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

The following types of tasks are performed on devices:

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

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

- *Group tasks*—Tasks that are performed on all devices of a specific group  
Unless otherwise specified in the task properties, a group task also affects all subgroups of the selected group. A group task also affects (optionally) devices that have been connected to secondary and virtual Administration Servers deployed in the group or any of its subgroups.
- *Global tasks*—Tasks that are performed on a set of devices, regardless of whether they are included in any group.

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

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

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

Execution results of tasks are saved in the operating system event log on each device, in the operating system event log on the Administration Server, and in the Administration Server database.

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

## About task scope

The *scope of a [task](#)* is the set of devices on which the task is performed. The types of scope are as follows:

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

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

- Specifying certain devices manually.  
You can use an IP address (or IP range) or DNS name as the device address.
- Importing a list of devices from a .txt file with the device addresses to be added (each address must be placed on an individual line).  
If you import a list of devices from a file or create a list manually, and if devices are identified by their names, the list can only contain devices for which information has already been entered into the Administration Server database. Moreover, the information must have been entered when those devices were connected or during device discovery.
- Specifying a device selection.  
Over time, the scope of a task changes as the set of devices included in the selection change. A selection of devices can be made on the basis of device attributes, including software installed on a device, and on the basis of tags assigned to devices. Device selection is the most flexible way to specify the scope of a task.  
Tasks for device selections are always run on a schedule by the Administration Server. These tasks cannot be run on devices that lack connection to the Administration Server. Tasks whose scope is specified by using other methods are run directly on devices and therefore do not depend on the device connection to the Administration Server.

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

## Creating a task

*To create a task:*

1. In the main menu, go to **Assets (Devices) → 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 modify 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:*

1. In the main menu, go to **Assets (Devices) → Managed devices**.

The list of managed devices is displayed.

2. In the list of managed devices, select check boxes next to the devices to run the task for them. You can use the search and filter functions to find the devices you're looking for.

3. Click the **Run task** button, and then select **Add a new task**.

The New task wizard starts.

On the first step of the wizard, you can remove the devices selected to include in the task scope. Follow the wizard instructions.

4. Click the **Finish** button.

The task is created for the selected devices.

## Starting a task manually

The application starts tasks according to the schedule settings specified in the properties of each task. You can start a task manually at any time from the task list. Alternatively, you can select devices in the **Managed devices** list, and then start an existing task for them.

*To start a task manually:*

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

## Viewing the task list

You can view the list of tasks that are created in Kaspersky Security Center Linux.

*To view the list of tasks,*

In the main menu, go to **Assets (Devices)** → **Tasks**.

The list of tasks is displayed. The tasks are grouped by the names of applications to which they are related. For example, the *Install application remotely* task is related to the Administration Server, and the *Update* task refers to Kaspersky Endpoint Security.

*To view properties of a task,*

Click the name of the task.

The task properties window is displayed with [several named tabs](#). For example, the **Task type** is displayed on the **General** tab, and the task schedule—on the **Schedule** tab.

## General task settings

This section contains the settings that you can view and configure for most of your tasks. The list of settings available depends on the task you are configuring.

### Settings specified during task creation

You can specify the following settings when creating a task. Some of these settings can also be modified in the properties of the created task.

- Operating system restart settings:

- [Do not restart the device](#) ?

Client devices are not restarted automatically after the operation. To complete the operation, you must restart a device (for example, manually or through a device management task). Information about the required restart is saved in the task results and in the device status. This option is suitable for tasks on servers and other devices where continuous operation is critical.

- [Restart the device](#) ?

Client devices are always restarted automatically if a restart is required for completion of the operation. This option is useful for tasks on devices that provide for regular pauses in their operation (shutdown or restart).

- [Force closure of applications in blocked sessions](#) 

Running applications may prevent a restart of the client device. For example, if a document is being edited in a word processing application and is not saved, the application does not allow the device to restart.

If this option is enabled, such applications on a locked device are forced to close before the device restart. As a result, users may lose their unsaved changes.

If this option is disabled, a locked device is not restarted. The task status on this device states that a device restart is required. Users have to manually close all applications running on locked devices and restart these devices.

By default, this option is disabled.

- Task scheduling settings:

- **Scheduled start setting:**

- [Every N hours](#) 

The task runs regularly, with the specified interval in hours, starting from the specified date and time. By default, the task runs every six 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.

- [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.

- [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 Security Center Linux.

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 week, at the specified time.  
By default, the task runs every Friday at 6:00:00 PM.

- [Monthly](#)

The task runs regularly, on the specified day of the month, at the specified time.  
In months that lack the specified day, the task runs on the last day.  
By default, the task runs on the first day of each month, at the current system time.

- [Manually](#)

The task does not run automatically. You can only start it manually.  
By default, this option is enabled.

- [Every month on specified days of selected weeks](#)

The task runs regularly, on the specified days of each month, at the specified time.  
By default, no days of month are selected; the default start time is 6:00:00 PM.

- [When new updates are downloaded to the repository](#)

The task runs after updates are downloaded to the repository. For example, you may want to use this schedule for the *Update* task.

- [On completing another task](#)

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. This parameter only works if both tasks are assigned to the same devices.

- [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**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- [Use automatically randomized delay for task starts](#) 

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However, when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- [Use randomized delay for task starts within an interval of \(min\)](#) 

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

- Devices to which the task will be assigned:

- [Select networked devices detected by Administration Server](#) 

The task is assigned to specific devices. The specific devices can include devices in administration groups as well as unassigned devices.

For example, you may want to use this option in a task of installing Network Agent on unassigned devices.

- [Specify device addresses manually or import addresses from list](#) 

You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

- [Assign task to a device selection](#) 

The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.

- [Assign task to an administration group](#) 

The task is assigned to devices included in an administration group. You can specify one of the existing groups or create a new one.

For example, you may want to use this option to run a task of sending a message to users if the message is specific for devices included in a specific administration group.

- Account settings:

- [Default account](#) 

The task will be run under the same account as the application that performs this task.

By default, this option is selected.

- [Specify an account](#) 

Fill in the **Account** and **Password** fields to specify the details of an account under which the task is run. The account must have sufficient rights for this task.

- [Account](#) 

Account under which the task is run.

- [Password](#) 

Password of the account under which the task will be run.

## Settings specified after task creation

You can specify the following settings only after a task is created.

- Group task settings:

- [Distribute to subgroups](#) 

This option is only available in the settings of the group tasks.

When this option is enabled, the [task scope](#) includes:

- The administration group that you selected while creating the task.
- The administration groups subordinate to the selected administration group at any level down by the [group hierarchy](#).

When this option is disabled, the task scope includes only the administration group that you selected while creating the task.

By default, this option is enabled.

- [Distribute to secondary and virtual Administration Servers](#) 

When this option is enabled, the task that is effective on the primary Administration Server is also applied on the secondary Administration Servers (including virtual ones). If a task of the same type already exists on the secondary Administration Server, both tasks are applied on the secondary Administration Server—the existing one and the one that is inherited from the primary Administration Server.

This option is only available when the **Distribute to subgroups** option is enabled.

By default, this option is disabled.

- Advanced scheduling settings:

- [Turn on devices by using the Wake-on-LAN function before starting the task \(min\)](#) 

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 complete, 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 \(min\)](#) 

After the specified time period expires, the task is stopped automatically, whether it is completed or not.

Enable this option if you want to interrupt (or stop) tasks that take too long to execute.

By default, this option is disabled. The default task execution time is 120 minutes.

- Notification settings:

- **Store task history** block:

- [Store in the Administration Server database for \(days\)](#) <sup>?</sup>

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](#) <sup>?</sup>

Application events related to execution of the task are stored locally in the Syslog Event Log of each client device.

By default, this option is disabled.

- [Store in the OS event log on Administration Server](#) <sup>?</sup>

Application events related to execution of the task on all client devices from the task scope are stored centrally in the Syslog Event Log of the Administration Server operating system (OS).

By default, this option is disabled.

- [Save all events](#) <sup>?</sup>

If this option is selected, all events related to the task are saved to the event logs.

- [Save events related to task progress](#) <sup>?</sup>

If this option is selected, only events related to the task execution are saved to the event logs.

- [Save only task execution results](#) <sup>?</sup>

If this option is selected, only events related to the task results are saved to the event logs.

- [Notify administrator of task execution results](#) <sup>?</sup>

You can select the methods by which administrators receive notifications about task execution results: by email, by SMS, and by running an executable file. To configure notification, click the **Settings** link.

By default, all notification methods are disabled.

- [Notify of errors only](#) <sup>?</sup>

If this option is enabled, administrators are only notified when a task execution completes with an error.

If this option is disabled, administrators are notified after every task execution completion.

By default, this option is enabled.

- Security settings.

- Task scope settings.

Depending on how the task scope is determined, the following settings are present:

- [Devices](#) 

If the scope of a task is determined by an administration group, you can view this group. No changes are available here. However, you can set **Exclusions from task scope**.

If the scope of a task is determined by a list of devices, you can modify this list by adding and removing devices.

- [Device selection](#) 

You can change the device selection to which the task is applied.

- [Exclusions from task scope](#) 

You can specify groups of devices to which the task is not applied. Groups to be excluded can only be subgroups of the administration group to which the task is applied.

- Revision history.

## Exporting a task

Kaspersky Security Center Linux allows you to save a task and its settings to a KLT file. You can use this KLT file to [import the saved task](#) both to Kaspersky Security Center Windows and Kaspersky Security Center Linux.

*To export a task:*

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

2. Select the check box next to the task that you want to export.

You cannot export multiple tasks at the same time. If you select more than one task, the **Export** button will be disabled. Administration Server tasks are also unavailable for export.

3. Click the **Export** button.

4. In the opened **Save as** window, specify the task file name and path. Click the **Save** button.

The **Save as** window is displayed only if you use Google Chrome, Microsoft Edge, or Opera. If you use another browser, the task file is automatically saved in the **Downloads** folder.

## Importing a task

Kaspersky Security Center Linux allows you to import a task from a KLT file. The KLT file contains the [exported task](#) and its settings.

*To import a task:*

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

- [Specify device addresses manually or import addresses from a list](#) 

You can specify DNS names, IP addresses, and IP subnets of devices to which you want to assign the task.

You may want to use this option to execute a task for a specific subnet. For example, you may want to install a certain application on devices of accountants or to scan devices in a subnet that is probably infected.

- [Assign task to a device selection](#) 

The task is assigned to devices included in a device selection. You can specify one of the existing selections.

For example, you may want to use this option to run a task on devices with a specific operating system version.

6. Specify the task scope.

7. Click the **Complete** button to finish the task import.

The notification with the import results appears. If the task is imported successfully, you can click the **Details** link to view the task properties.

After a successful import, the task is displayed in the task list. The task settings and schedule are also imported. The task will be started according to its schedule.

If the newly imported task has an identical name to an existing task, the name of the imported task is expanded with the (<next sequence number>) index, for example: (1), (2).

## Starting the Change tasks password wizard

For a non-local task, you can specify an account under which the task must be run. You can specify the account during task creation or in the properties of an existing task. If the specified account is used in accordance with security instructions of the organization, these instructions might require changing the account password from time to time. When the account password expires and you set a new one, the tasks will not start until you specify the new valid password in the task properties.

The Change tasks password wizard enables you to automatically replace the old password with the new one in all tasks in which the account is specified. Alternatively, you can change this password manually in the properties of each task.

*To start the Change tasks password wizard:*

1. In the main menu, go to **Assets (Devices) → Tasks**.
2. Click **Manage credentials of accounts for starting tasks**.

Follow the instructions of the wizard.

## Step 1. Specifying credentials

Specify new credentials that are currently valid in your system. When you switch to the next step of the wizard, Kaspersky Security Center Linux checks if the specified account name matches the account name in the properties of each non-local task. If the account names match, the password in the task properties will be automatically replaced with the new one.

To specify the new account, select an option:

- [Use current account](#) 

The wizard uses the name of the account under which you are currently signed in to Kaspersky Security Center Web Console. Then manually specify the account password in the **Current password to use in tasks** field.

- [Specify a different account](#) 

Specify the name of the account under which the tasks must be started. Then specify the account password in the **Current password to use in tasks** field.



If you fill in the **Previous password (optional; if you want to replace it with the current one)** field, Kaspersky Security Center Linux replaces the password only for those tasks in which both the account name and the old password are found. The replacement is performed automatically. In all other cases you have to choose an action to take in the next step of the wizard.

## Step 2. Selecting an action to take

If you did not specify the previous password in the first step of the wizard or if the specified old password has not matched the passwords in the task properties, you must choose an action to take for the tasks found.

*To choose an action for a task:*

1. Select the check box next to the task for which you want to choose an action.
2. Perform one of the following:
  - To remove the password in the task properties, click **Delete credentials**.  
The task is switched to run under the default account.
  - To replace the password with a new one, click **Enforce the password change even if the old password is wrong or not provided**.
  - To cancel the password change, click **No action is selected**.

The chosen actions are applied after you move to the next step of the wizard.

## Step 3. Viewing the results

On the last step of the wizard, view the results for each of the found tasks. To complete the wizard, click the **Finish** button.

## Viewing task run results stored on the Administration Server

Kaspersky Security Center Linux allows you to view the results for group tasks, tasks for specific devices, and Administration Server tasks. No run results can be viewed for local 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.

## Application tags

This section describes application tags, and provides instructions for creating and modifying them as well as for tagging third-party applications.

## About application tags

Kaspersky Security Center Linux enables you to tag third-party applications (applications made by software vendors other than Kaspersky). 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 the 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 the 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.

## Granting offline access to the external device blocked by Device Control

In Device Control component of the Kaspersky Endpoint Security policy, you can manage user access to external devices that are installed on or connected to the client device (for example, hard drives, cameras, or Wi-Fi modules). This lets you protect the client device from infection when such external devices are connected, and prevent loss or leaks of data.

If you need to grant temporary access to the external device blocked by Device Control but it is not possible to add the device to the list of trusted devices, you can grant temporary offline access to the external device. Offline access means that the client device has no access to the network.

You can grant offline access to the external device blocked by Device Control only if the **Allow request for temporary access** option is enabled in the settings of the Kaspersky Endpoint Security policy, in the **Application settings** → **Security Controls** → **Device Control** section.

Granting offline access to the external device blocked by Device Control includes the following stages:

1. In the Kaspersky Endpoint Security dialog window, device user who wants to have access to the blocked external device, generates a request access file and sends it to the Kaspersky Security Center Linux administrator.
2. Getting this request, the Kaspersky Security Center Linux administrator creates an access key file and send it to the device user.
3. In the Kaspersky Endpoint Security dialog window, the device user activates the access key file and obtains temporary access to the external device.

*To grant temporary access to the external device blocked by Device Control:*

1. In the main menu, go to **Assets (Devices)** → **Managed devices**.  
The list of managed devices is displayed.
2. In this list, select the user's device that requests access to the external device blocked by Device Control.  
You can select only one device.
3. Above the list of managed devices, click the ellipsis button ( ... ), and then click the **Grant access to the device in offline mode** button.
4. In the **Application settings** window that opens, in the **Device Control** section, click the **Browse** button.
5. Select the request access file that you have received from the user, and then click the **Open** button. The file should have the AKEY format.  
The details of the locked device to which the user has requested access is displayed.
6. Specify the value of the **Access duration** setting.  
This setting defines the length of time for which you grant the user access to the locked device. The default value is the value that was specified by the user when creating the request access file.

7. Specify the value of the **Activation period** setting.

This setting defines the time period during which the user can activate access to the blocked device by using the provided access key.

8. Click the **Save** button.

9. In the window that opens, select the destination folder in which you want to save the file containing the access key for the blocked device.

10. Click the **Save** button.

As a result, when you send the user the access key file and the user activates it in the Kaspersky Endpoint Security dialog window, the user has temporary access to the blocked device for the specific period.

## Using the klscflag utility to open port 13291

Port 13291 on the Administration Server is used for receiving connections from the MMC-based Administration Console. On non-Windows computers, this port is closed by default.

If you want to allow connection to the MMC-based Administration Console or use the klakout utility, you can open this port by using the klscflag utility. Please note that the functionality of the MMC-based Administration Console is reduced when it is connected to Kaspersky Security Center Linux. We recommend that you use the Kaspersky Security Center Web Console to connect to Kaspersky Security Center Linux.

The klscflag utility changes the value of the KLSRV\_SP\_SERVER\_SSL\_PORT\_GUI\_OPEN parameter.

We recommend that you use Kaspersky Security Center Web Console to connect to Kaspersky Security Center Linux.

*To open port 13291:*

1. Execute the following command in the command line:

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
\"SS_SETTINGS\";"
```

2. Restart the Kaspersky Security Center Administration Server service by executing the following command:

```
$ sudo systemctl restart kladminserver_srv
```

Port 13291 is open.

*To check if port 13291 has been successfully open:*

Execute the following command in the command line:

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

This command returns the following result:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T>true
```

The true value means that the port is open. Otherwise, the false value is displayed.

## Registering Kaspersky Industrial CyberSecurity for Networks application in Kaspersky Security Center Web Console

To start working with the Kaspersky Industrial CyberSecurity for Networks application via Kaspersky Security Center Web Console, you must first register it in Kaspersky Security Center Web Console.

To register the Kaspersky Industrial CyberSecurity for Networks application:

1. Make sure that the following is done:

- You have [downloaded and installed the Kaspersky Industrial CyberSecurity for Networks web plug-in](#).  
You can do it later while waiting for the Kaspersky Industrial CyberSecurity for Networks Server to synchronize with the Administration Server. After the plug-in is downloaded and installed, the **KICS for Networks** section is displayed in the Kaspersky Security Center Web Console main menu.
- In the Kaspersky Industrial CyberSecurity for Networks web interface, interaction with Kaspersky Security Center is configured and enabled. For details, refer to the [Kaspersky Industrial CyberSecurity for Networks Online Help](#).

2. Move the device where Kaspersky Industrial CyberSecurity for Networks Server is installed from the Unassigned devices group to the Managed devices group:

- a. In the main menu, go to **Discovery & deployment** → **Unassigned devices**.
- b. Select the check box next to the device where the Kaspersky Industrial CyberSecurity for Networks Server is installed.
- c. Click the **Move to group** button.
- d. In the hierarchy of administration groups, select the check box next to the **Managed devices** group.
- e. Click the **Move** button.

3. Open the properties window of the device where the Kaspersky Industrial CyberSecurity for Networks Server is installed.

4. On the device properties page, in the **General** section, select the **Do not disconnect from the Administration Server** option, and then click the **Save** button.

5. On the device properties page, select the **Applications** section.

6. In the **Applications** section, select Kaspersky Security Center Network Agent.

7. If the current status of the application is *Stopped*, wait until it changes to *Running*.

This may take up to 15 minutes. If you have not yet installed the Kaspersky Industrial CyberSecurity for Networks web plug-in, you can do it now.

8. If you want to view the statistics of Kaspersky Industrial CyberSecurity for Networks, you may add widgets on the dashboard. To add the widgets, do the following:

- a. In the main menu, go to **Monitoring & Reporting** → **Dashboard**.

- b. On the dashboard, click the **Add or restore web widget** button.
  - c. In the widget menu that opens, select **Other**.
  - d. Select the widgets that you want to add:
    - KICS for Networks deployment map
    - Information about KICS for Networks Servers
    - Up-to-date events of KICS for Networks
    - Devices with issues in KICS for Networks
    - Critical events in KICS for Networks
    - Statuses in KICS for Networks
9. To proceed to the Kaspersky Industrial CyberSecurity for Networks web interface, do the following:
- a. In the main menu, go to **KICS for Networks** → **Search**.
  - b. Click the **Find events or devices** button.
  - c. In the **Query parameters** window that opens, click the **Server** field.
  - d. Select the Kaspersky Industrial CyberSecurity for Networks Server from the drop-down list of servers that are integrated with Kaspersky Security Center, and then click the **Find** button.
  - e. Click the **Go to Server** link next to the name of the Kaspersky Industrial CyberSecurity for Networks Server. The Kaspersky Industrial CyberSecurity for Networks sign-in page is displayed.

To log in to the Kaspersky Industrial CyberSecurity for Networks web interface, you need to provide the application user account credentials.

# Managing users and user roles

This section describes users and user roles, and provides instructions for creating and modifying them, for assigning roles and groups to users, and for associating policy profiles with roles.

## About user accounts

Kaspersky Security Center Linux allows you to manage user accounts and security groups. The application supports two types of accounts:

- Accounts of organization employees. Administration Server retrieves data of the accounts of those local users when polling the organization's network.
- Accounts of internal users of Kaspersky Security Center Linux. You can create accounts of internal users on the portal. These accounts are used only within Kaspersky Security Center Linux.

*To view tables of user accounts and security groups:*

1. In the main menu, go to **Users & roles** → **Users & groups**.
2. Select the **Users** or the **Groups** tab.

The table of users or security groups opens. If you want to view the table with only internal users or groups or with only local users or groups, set the **Subtype** filter criteria to **Internal** or **Local** respectively.

## 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 functions that require different security settings is considerably smaller.

## Differences from using policy profiles

Policy profiles are properties of a policy that is created for each Kaspersky application separately. A role is associated with many policy profiles created for different applications. Therefore, a role is a method of uniting settings for a certain user type in one place.

## Configuring access rights to application features. Role-based access control

Kaspersky Security Center Linux provides facilities for role-based access to the features of Kaspersky Security Center Linux and managed Kaspersky applications.

You can configure [access rights to application features](#) for Kaspersky Security Center Linux users in one of the following ways:

- By configuring the rights for each user or group of users individually.
- By creating standard [user roles](#) with a predefined set of rights and assigning those roles to users depending on their scope of duties.

Application of user roles is intended to simplify and shorten routine procedures of configuring users' access rights to application features. Access rights within a role are configured in accordance with the standard tasks and the users' scope of duties.

User roles can be assigned names that correspond to their respective purposes. You can create an unlimited number of roles in the application.

You can use the [predefined user roles](#) with already configured set of rights, or [create new roles](#) and configure the required rights yourself.

## Access rights to application features

The table below shows the Kaspersky Security Center Linux features with the access rights to manage the associated tasks, reports, settings, and perform the associated user actions.

To perform the user actions listed in the table, a user has to have the right specified next to the action.

**Read**, **Write**, and **Execute** rights are applicable to any task, report, or setting. In addition to these rights, a user has to have the **Perform operations on device selections** right to manage tasks, reports, or settings on device selections.

All tasks, reports, settings, and installation packages that are missing in the table belong to the **General features: Basic functionality** functional area.

| Functional area                                                                     | Right                                                                                                                                                                       | User action: right required to perform the action                                                                                                                                                                                                                                                                                                          | Task                                                                                                                                                                                                                                                                   | Report                                                                                                                                                                                                                                                    | Other       |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| <p><b>General features:</b><br/> <b>Management of administration groups</b></p>     | <p><b>Write</b></p>                                                                                                                                                         | <ul style="list-style-type: none"> <li>• Add device to an administration group: <b>Write</b></li> <li>• Delete device from an administration group: <b>Write</b></li> <li>• Add an administration group to another administration group: <b>Write</b></li> <li>• Delete an administration group from another administration group: <b>Write</b></li> </ul> | <p>None</p>                                                                                                                                                                                                                                                            | <p>None</p>                                                                                                                                                                                                                                               | <p>None</p> |
| <p><b>General features:</b><br/> <b>Access objects regardless of their ACLs</b></p> | <p><b>Read</b></p>                                                                                                                                                          | <p>Get read access to all objects:<br/> <b>Read</b></p>                                                                                                                                                                                                                                                                                                    | <p>None</p>                                                                                                                                                                                                                                                            | <p>None</p>                                                                                                                                                                                                                                               | <p>None</p> |
| <p><b>General features:</b><br/> <b>Basic functionality</b></p>                     | <ul style="list-style-type: none"> <li>• <b>Read</b></li> <li>• <b>Write</b></li> <li>• <b>Execute</b></li> <li>• <b>Perform operations on device selections</b></li> </ul> | <ul style="list-style-type: none"> <li>• Device moving rules (create, modify, or delete) for the virtual Server: <b>Write, Perform operations on device selections</b></li> <li>• Get Mobile (LWNGT) protocol custom certificate: <b>Read</b></li> <li>• Set Mobile (LWNGT) protocol custom</li> </ul>                                                     | <ul style="list-style-type: none"> <li>• "Download updates to the Administration Server repository"</li> <li>• "Deliver reports"</li> <li>• "Distribute installation package"</li> <li>• "Install application on secondary Administration Servers remotely"</li> </ul> | <ul style="list-style-type: none"> <li>• "Report on protection status"</li> <li>• "Report on threats"</li> <li>• "Report on most heavily infected devices"</li> <li>• "Report on status of anti-virus databases"</li> <li>• "Report on errors"</li> </ul> | <p>None</p> |

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 operating system log:  
**Read**

- "Report on network attacks"
- "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"
- "Report on prohibited applications"
- "Report on Web Control"
- "Report on encryption status of managed devices"

|                                                     |                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                    |      |                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                         |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                     |                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                    |      | <ul style="list-style-type: none"> <li>• "Report on encryption status of mass storage devices"</li> <li>• "Report on rights to access encrypted drives"</li> <li>• "Report on file encryption errors"</li> <li>• "Report on blockage of access to encrypted files"</li> <li>• "Report on effective user permissions"</li> <li>• "Report on rights"</li> </ul> |                                                                                                                                                                                         |
| <b>General features:</b><br><b>Deleted objects</b>  | <ul style="list-style-type: none"> <li>• <b>Read</b></li> <li>• <b>Write</b></li> </ul>                                                                                                           | <ul style="list-style-type: none"> <li>• View deleted objects in the Recycle Bin:<br/><b>Read</b></li> <li>• Delete objects from the Recycle Bin:<br/><b>Write</b></li> </ul>                                                                                      | None | None                                                                                                                                                                                                                                                                                                                                                          | None                                                                                                                                                                                    |
| <b>General features:</b><br><b>Event processing</b> | <ul style="list-style-type: none"> <li>• <b>Delete events</b></li> <li>• <b>Edit event notification settings</b></li> <li>• <b>Edit event logging settings</b></li> <li>• <b>Write</b></li> </ul> | <ul style="list-style-type: none"> <li>• Change events registration settings: <b>Edit event logging settings</b></li> <li>• Change events notification settings: <b>Edit event notification settings</b></li> <li>• Delete events: <b>Delete events</b></li> </ul> | None | None                                                                                                                                                                                                                                                                                                                                                          | <b>Settings:</b> <ul style="list-style-type: none"> <li>• The maximum number of events stored the database</li> <li>• Period time for storing events from the deleted device</li> </ul> |

|                                                                         |                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                               |             |             |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|
| <p><b>General features:<br/>Operations on Administration Server</b></p> | <ul style="list-style-type: none"> <li>• <b>Read</b></li> <li>• <b>Write</b></li> <li>• <b>Execute</b></li> <li>• <b>Modify object ACLs</b></li> <li>• <b>Perform operations on device selections</b></li> </ul> | <ul style="list-style-type: none"> <li>• Specify ports of Administration Server for the network agent connection:<br/><b>Write</b></li> <li>• Specify ports of Activation Proxy launched on the Administration Server: <b>Write</b></li> <li>• Specify ports of Activation Proxy for Mobile launched on the Administration Server: <b>Write</b></li> <li>• Specify ports of the Web Server for distribution of standalone packages: <b>Write</b></li> <li>• Specify ports of the Web Server for distribution of MDM profiles: <b>Write</b></li> <li>• Specify SSL-ports of the Administration Server for connection via Web Console: <b>Write</b></li> <li>• Specify ports of the Administration Server for mobile connection: <b>Write</b></li> <li>• Specify the maximum number of</li> </ul> | <ul style="list-style-type: none"> <li>• "Backup of Administration Server data"</li> <li>• "Databases maintenance"</li> </ul> | <p>None</p> | <p>None</p> |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|

|                                                               |                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                         |      |                                                                                                                                                                                                                                                                                                                                |                                             |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
|                                                               |                                                                                                                                                                                                              | <p>events stored in the Administration Server database:<br/><b>Write</b></p> <ul style="list-style-type: none"> <li>Specify the maximum number of events that can be sent by the Administration Server: <b>Write</b></li> <li>Specify time period during which events can be sent by the Administration Server: <b>Write</b></li> </ul> |      |                                                                                                                                                                                                                                                                                                                                |                                             |
| <p><b>General features: Kaspersky software deployment</b></p> | <ul style="list-style-type: none"> <li><b>Manage Kaspersky patches</b></li> <li><b>Read</b></li> <li><b>Write</b></li> <li><b>Execute</b></li> <li><b>Perform operations on device selections</b></li> </ul> | <p>Approve or decline installation of the patch:<br/><b>Manage Kaspersky patches</b></p>                                                                                                                                                                                                                                                | None | <ul style="list-style-type: none"> <li>"Report on license key usage by virtual Administration Server"</li> <li>"Report on Kaspersky software versions"</li> <li>"Report on incompatible applications"</li> <li>"Report on versions of Kaspersky software module updates"</li> <li>"Report on protection deployment"</li> </ul> | <p>Installation package:<br/>"Kaspersk"</p> |
| <p><b>General features: Key management</b></p>                | <ul style="list-style-type: none"> <li><b>Export key file</b></li> <li><b>Write</b></li> </ul>                                                                                                               | <ul style="list-style-type: none"> <li>Export key file:<br/><b>Export key file</b></li> <li>Modify Administration</li> </ul>                                                                                                                                                                                                            | None | None                                                                                                                                                                                                                                                                                                                           | None                                        |

|                                                          |                                                                                         |                                                                                                                                                                                                                                                                                                                                                                   |      |      |      |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
|                                                          |                                                                                         | Server license key settings:<br><b>Write</b>                                                                                                                                                                                                                                                                                                                      |      |      |      |
| General features:<br>Enforced report management          | <ul style="list-style-type: none"> <li>• <b>Read</b></li> <li>• <b>Write</b></li> </ul> | <ul style="list-style-type: none"> <li>• Create reports regardless of their ACLs:<br/><b>Write</b></li> <li>• Execute reports regardless of their ACLs:<br/><b>Read</b></li> </ul>                                                                                                                                                                                | None | None | None |
| General features:<br>Hierarchy of Administration Servers | Configure hierarchy of Administration Servers                                           | <ul style="list-style-type: none"> <li>• Register, update, or delete secondary Administration Servers:<br/><b>Configure hierarchy of Administration Servers</b></li> </ul>                                                                                                                                                                                        | None | None | None |
| General features: User permissions                       | Modify object ACLs                                                                      | <ul style="list-style-type: none"> <li>• Change Security properties of any object:<br/><b>Modify object ACLs</b></li> <li>• Manage user roles: <b>Modify object ACLs</b></li> <li>• Manage internal users: <b>Modify object ACLs</b></li> <li>• Manage security groups: <b>Modify object ACLs</b></li> <li>• Manage aliases: <b>Modify object ACLs</b></li> </ul> | None | None | None |
| General features:<br>Virtual                             | <ul style="list-style-type: none"> <li>• <b>Manage virtual</b></li> </ul>               | <ul style="list-style-type: none"> <li>• Get list of virtual</li> </ul>                                                                                                                                                                                                                                                                                           | None | None | None |

|                                                       |                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                         |                              |      |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|------------------------------|------|
| Administration Servers                                | <b>Administration Servers</b> <ul style="list-style-type: none"> <li>• <b>Read</b></li> <li>• <b>Write</b></li> <li>• <b>Execute</b></li> <li>• <b>Perform operations on device selections</b></li> </ul> | Administration Servers: <b>Read</b> <ul style="list-style-type: none"> <li>• Get information on the virtual Administration Server: <b>Read</b></li> <li>• Create, update, or delete a virtual Administration Server: <b>Manage virtual Administration Servers</b></li> <li>• Move a virtual Administration Server to another group: <b>Manage virtual Administration Servers</b></li> <li>• Set administration virtual Server permissions: <b>Manage virtual Administration Servers</b></li> </ul> |                                                                                                                                         |                              |      |
| General features: Encryption Key Management           | <b>Write</b>                                                                                                                                                                                              | Import the encryption keys: <b>Write</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                           | None                                                                                                                                    | None                         | None |
| System management: Vulnerability and patch management | <ul style="list-style-type: none"> <li>• <b>Read</b></li> <li>• <b>Write</b></li> <li>• <b>Execute</b></li> <li>• <b>Perform operations on device selections</b></li> </ul>                               | <ul style="list-style-type: none"> <li>• View third-party patch properties: <b>Read</b></li> <li>• Change third-party patch properties: <b>Write</b></li> </ul>                                                                                                                                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• "Fix vulnerabilities"</li> <li>• "Install required updates and fix vulnerabilities"</li> </ul> | "Report on software updates" | None |



## Predefined user roles

User roles assigned to Kaspersky Security Center Linux users provide them with sets of access rights to application features.

Users created on a virtual Server cannot be assigned a role on the Administration Server.

You can use the predefined user roles with already configured set of rights, or create new roles and configure the required rights yourself. Some of the predefined user roles available in Kaspersky Security Center Linux can be associated with specific job positions, for example, **Auditor**, **Security Officer**, **Supervisor**. Access rights of these roles are pre-configured in accordance with the standard tasks and scope of duties of the associated positions. The table below shows how roles can be associated with specific job positions.

Examples of roles for specific job positions

| Role             | Comment                                                                                                                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auditor          | Permits all operations with all types of reports, all viewing operations, including viewing deleted objects (grants the <b>Read</b> and <b>Write</b> permissions in the <b>Deleted objects</b> area). Does not permit other operations. You can assign this role to a person who performs the audit of your organization. |
| 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 <b>System management: Connectivity</b> 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.

Features of the functional areas **Mobile Device Management: General** and **System management** are not available in Kaspersky Security Center Linux. A user with the roles **Vulnerability and patch management administrator/operator** or **Mobile Device Management Administrator/Operator** has access only for rights from the **General features: Basic functionality** area.

Access rights of predefined user roles

| Role                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administration Server Administrator | Permits all operations in the following functional areas, in <b>General features</b> : <ul style="list-style-type: none"><li>• <b>Basic functionality</b></li><li>• <b>Event processing</b></li><li>• <b>Hierarchy of Administration Servers</b></li><li>• <b>Virtual Administration Servers</b></li></ul> Grants the <b>Read</b> and <b>Write</b> rights in the <b>General features: Encryption key management</b> functional area. |
| Administration Server Operator      | Grants the <b>Read</b> and <b>Execute</b> rights in all of the following functional areas, in <b>General features</b> : <ul style="list-style-type: none"><li>• <b>Basic functionality</b></li></ul>                                                                                                                                                                                                                                 |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | <ul style="list-style-type: none"> <li>• <b>Virtual Administration Servers</b></li> </ul>                                                                                                                                                                                                                                                                                                                |
| Auditor                                   | <p>Permits all operations in the following functional areas, in <b>General features</b>:</p> <ul style="list-style-type: none"> <li>• <b>Access objects regardless of their ACLs</b></li> <li>• <b>Deleted objects</b></li> <li>• <b>Enforced report management</b></li> </ul> <p>You can assign this role to a person who performs the audit of your organization.</p>                                  |
| Installation Administrator                | <p>Permits all operations in the following functional areas, in <b>General features</b>:</p> <ul style="list-style-type: none"> <li>• <b>Basic functionality</b></li> <li>• <b>Kaspersky software deployment</b></li> <li>• <b>License key management</b></li> </ul> <p>Grants <b>Read</b> and <b>Execute</b> rights in the <b>General features: Virtual Administration Servers</b> functional area.</p> |
| Installation Operator                     | <p>Grants the <b>Read</b> and <b>Execute</b> rights in all of the following functional areas, in <b>General features</b>:</p> <ul style="list-style-type: none"> <li>• <b>Basic functionality</b></li> <li>• <b>Kaspersky software deployment</b> (also grants the <b>Manage Kaspersky Lab patches</b> right in this area)</li> <li>• <b>Virtual Administration Servers</b></li> </ul>                   |
| Kaspersky Endpoint Security Administrator | <p>Permits all operations in the following functional areas:</p> <ul style="list-style-type: none"> <li>• <b>General features: Basic functionality</b></li> <li>• Kaspersky Endpoint Security area, including all features</li> </ul> <p>Grants the <b>Read</b> and <b>Write</b> rights in the <b>General features: Encryption key management</b> functional area.</p>                                   |
| Kaspersky Endpoint Security Operator      | <p>Grants the <b>Read</b> and <b>Execute</b> rights in all of the following functional areas:</p> <ul style="list-style-type: none"> <li>• <b>General features: Basic functionality</b></li> <li>• Kaspersky Endpoint Security area, including all features</li> </ul>                                                                                                                                   |
| Main Administrator                        | <p>Permits all operations in functional areas, <i>except</i> for the following areas, in <b>General features</b>:</p> <ul style="list-style-type: none"> <li>• <b>Access objects regardless of their ACLs</b></li> <li>• <b>Enforced report management</b></li> </ul> <p>Grants the <b>Read</b> and <b>Write</b> rights in the <b>General features: Encryption key management</b> functional area.</p>   |
| Main Operator                             | <p>Grants the <b>Read</b> and <b>Execute</b> (where applicable) rights in all of the following functional areas:</p>                                                                                                                                                                                                                                                                                     |

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        | <ul style="list-style-type: none"> <li>• <b>General features:</b></li> <li>• <b>Basic functionality</b></li> <li>• <b>Deleted objects</b></li> <li>• <b>Operations on Administration Server</b></li> <li>• <b>Kaspersky Lab software deployment</b></li> <li>• <b>Virtual Administration Servers</b></li> <li>• Kaspersky Endpoint Security area, including all features</li> </ul>                                                                                                                                                                                               |
| Mobile Device Management Administrator | Permits all operations in the <b>General features: Basic functionality</b> functional area.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Security Officer                       | <p>Permits all operations in the following functional areas, in <b>General features:</b></p> <ul style="list-style-type: none"> <li>• <b>Access objects regardless of their ACLs</b></li> <li>• <b>Enforced report management</b></li> </ul> <p>Grants the <b>Read, Write, Execute, Save files from devices to the administrator's workstation</b>, and <b>Perform operations on device selections</b> rights in the <b>System management: Connectivity</b> functional area.</p> <p>You can assign this role to an officer in charge of the IT security in your organization.</p> |
| Self Service Portal User               | Permits all operations in the <b>Mobile Device Management: Self Service Portal</b> functional area. This feature is not supported in Kaspersky Security Center 11 and later version.                                                                                                                                                                                                                                                                                                                                                                                              |
| Supervisor                             | <p>Grants the <b>Read</b> right in the <b>General features: Access objects regardless of their ACLs</b> and <b>General features: Enforced report management</b> functional areas.</p> <p>You can assign this role to a security officer and other managers in charge of the IT security in your organization.</p>                                                                                                                                                                                                                                                                 |

## 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:

- **Assets (Devices) → Hierarchy of groups**
- **Assets (Devices) → Tasks**
- **Monitoring & reporting → Reports**
- **Assets (Devices) → Device selections**
- **Monitoring & reporting → 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 groups

You can give users and groups access rights to use different features of Administration Server and of the Kaspersky applications for which you have management plug-ins, for example, Kaspersky Endpoint Security for Linux.

*To assign access rights to a user or a group of users:*

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 **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 (only for Kaspersky Security Center Linux 11 or later)
  - Access objects regardless of their ACLs (only for Kaspersky Security Center Linux 11 or later)
  - Basic functionality
  - Deleted objects (only for Kaspersky Security Center Linux 11 or later)
  - Encryption Key Management
  - Event processing
  - Operations on Administration Server (only in the property window of Administration Server)
  - Kaspersky software 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
  - Hardware inventory
  - Network Access Control
  - Operating system deployment
  - Remote installation
  - Software inventory

If neither **Allow** nor **Deny** is selected for an access right, then the access right 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.

## Adding an account of an internal user

*To add a new internal user account to Kaspersky Security Center Linux:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click **Add**.
3. In the **Add user** window that opens, specify the settings of the new user account:
  - **Name**.
  - **Password** for the user connection to Kaspersky Security Center Linux.  
The password must comply with the following rules:
    - The password must be 8 to 16 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 "@".

To see the characters that you entered, click and hold the **Show** button.

The number of attempts for entering the password is limited. By default, the maximum number of allowed password entry attempts is 10. You can change the allowed number of attempts to enter a password, as described in "[Changing the number of allowed password entry attempts](#)".

If the user enters an invalid password the specified number of times, the user account is blocked for one hour. You can unblock the user account only by changing the password.

4. Click **Save** to save the changes.

A new user account is added to the user list.

## 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 **Add**.
3. In the **Create security group** window that opens, specify the following settings for the new security group:

- **Group name**
- **Description**

4. Click **Save** to save the changes.

A new security group is added to the group list.

## Editing an account of an internal user

*To edit an internal user account in Kaspersky Security Center Linux:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the name of the user account that you want to edit.
3. In the user settings window that opens, on the **General** tab, change the settings of the user account:

- **Description**
- **Full name**
- **Email address**
- **Main phone**
- **Set new password** for the user connection to Kaspersky Security Center Linux.

The password must comply with the following rules:

- The password must be 8 to 16 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 "@".

To see the entered password, click and hold the **Show** button.

The number of attempts for entering the password is limited. By default, the maximum number of allowed password entry attempts is 10. You can [change](#) the allowed number of attempts; however, for security reasons, we do not recommend that you decrease this number. If the user enters an invalid password the specified number of times, the user account is blocked for one hour. You can unblock the user account only by changing the password.

- If necessary, switch the toggle button to **Disabled** to prohibit the user from connecting to the application. You can disable an account, for example, after an employee leaves the company.
4. On the **Authentication security** tab, you can specify the security settings for this account.
  5. On the **Groups** tab, you can add the user to security groups.
  6. On the **Devices** tab, you can [assign devices](#) to the user.
  7. On the **Roles** tab, you can [assign roles](#) to the user.
  8. Click **Save** to save the changes.

The updated user account appears in the list of users.

## Editing a security group



*To edit a security group:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Groups** tab.
2. Click the name of the security group that you want to edit.
3. In the group settings window that opens, change the settings of the security group:
  - On the **General** tab, you can change the **Name** and **Description** settings. These settings are available only for internal security groups.
  - On the **Users** tab, you can [add users to the security group](#). This setting is available only for internal users and internal security groups.
  - On the **Roles** tab, you can [assign a role](#) to the security group.
4. Click **Save** to save the changes.

The changes are applied to the security group.

## Assigning a role to a user or a security group

*To assign a role to a user or a security group:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** or the **Groups** tab.
2. Select the name of the user or the security group to whom to assign a role.  
You can select multiple names.
3. On the menu line, click the **Assign role** button.  
The Role assignment wizard starts.
4. Follow the instructions of the wizard: select the role that you want to assign to the selected users or security groups, and then select the scope of role.  
*A user role scope is a combination of users and administration groups. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.*

The role with a set of rights for working with Administration Server is assigned to the user (or users, or the security group). In the list of users or security groups, a check box appears in the **Has assigned roles** column.

## Adding user accounts to an internal security group

You can add only accounts of internal users to an internal security group.

*To add user accounts to an internal security group:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.

2. Select check boxes next to user accounts that you want to add to a security group.
3. Click the **Assign group** button.
4. In the **Assign group** window that opens, select the security group to which you want to add user accounts.
5. Click the **Save** button.

The user accounts are added to the security group. You can also add internal users to a security group by using the [group settings](#).

## Assigning a user as a device owner

For information about assigning a user as a mobile device owner, see [Kaspersky 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.

A 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 **Assets (Devices)** → **Managed devices**, by clicking the name of the device that you want to assign, and then clicking the **Manage device owner** link.

## Enabling account protection from unauthorized modification

You can enable an additional option to protect a user account from unauthorized modification. If this option is enabled, modifying user account settings requires authorization of the user with the rights for modification.

To enable or disable account protection from unauthorized modification:

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the name of the internal user account for which you want to specify account protection from unauthorized modification.
3. In the user settings window that opens, select the **Authentication security** tab.
4. On the **Authentication security** tab, select the **Request authentication to check for permission to modify this account** option if you want to request credentials every time when account settings are changed or modified. Otherwise, select the **Allow users to modify this account without additional authentication** option.
5. Click the **Save** button.

## Two-step verification

This section describes how you can use two-step verification to reduce the risk of unauthorized access to Kaspersky Security Center Web Console.

## Scenario: configuring two-step verification for all users

This scenario describes how to enable two-step verification for all users and how to exclude user accounts from two-step verification. If you did not enable two-step verification for your account before you enable it for other users, the application opens the window for enabling two-step verification for your account, first. This scenario also describes how to enable two-step verification for your own account.

If you enabled two-step verification for your account, you may proceed to the stage of enabling of two-step verification for all users.

### Prerequisites

Before you start:

- Make sure that your user account has the Modify object ACLs right of the **General features: User permissions** functional area for modifying security settings for other users' accounts.
- Make sure that the other users of Administration Server install an authenticator application on their devices.

### Stages

Enabling two-step verification for all users proceeds in stages:

#### 1 Installing an authenticator application on a device

You can install any application that supports the Time-based One-time Password algorithm (TOTP), such as:

- Google Authenticator

- Microsoft Authenticator
- Bitrix24 OTP
- Yandex Key
- Avanpost Authenticator
- Aladdin 2FA

To check if Kaspersky Security Center Linux supports the authenticator application that you want to use, enable two-step verification for all users or for a particular user.

One of the steps suggests that you specify the security code generated by the authenticator application. If it succeeds, then Kaspersky Security Center Linux supports the selected authenticator.

## 2 Synchronizing the authenticator application time with the time of the device on which Administration Server is installed

Ensure that the time on the device with the authenticator application and the time on the device with the Administration Server are synchronized to UTC, by using external time sources. Otherwise, failures may occur during the authentication and activation of two-step verification.

## 3 Enabling two-step verification for your account and receiving the secret key for your account

After you [enable two-step verification for your account](#), you can enable two-step verification for all users.

## 4 Enabling two-step verification for all users

Users [with two-step verification enabled](#) must use it to log in to Administration Server.

## 5 Prohibit new users from setting up two-step verification for themselves

In order to further improve Kaspersky Security Center Web Console access security, you can [prohibit new users from setting up two-step verification for themselves](#).

## 6 Editing the name of a security code issuer

If you have several Administration Servers with similar names, [you may have to change the security code issuer names](#) for better recognition of different Administration Servers.

## 7 Excluding user accounts for which you do not need to enable two-step verification

If required, [you can exclude users from two-step verification](#). Users with excluded accounts do not have to use two-step verification to log in to Administration Server.

## 8 Configuring two-step verification for your own account

If the users are not excluded from two-step verification and two-step verification is not yet configured for their accounts, [they need to configure it](#) in the window that opens when they sign-in to Kaspersky Security Center Web Console. Otherwise, they will not be able to access the Administration Server in accordance with their rights.

## Results

Upon completion of this scenario:

- Two-step verification is enabled for your account.
- Two-step verification is enabled for all user accounts of the Administration Server, except for user accounts that were excluded.

## About two-step verification for an account

Kaspersky Security Center Linux provides two-step verification for users of Kaspersky Security Center Web Console. When two-step verification is enabled for your own account, every time you log in to Kaspersky Security Center Web Console, you enter your user name, password, and an additional single-use security code. To receive a single-use security code, you must have an authenticator app on your computer or your mobile device.

A security code has an identifier referred to as *issuer name*. The security code issuer name is used as an identifier of the Administration Server in the authenticator app. You can change the name of the security code issuer name. The security code issuer name has a default value that is the same as the name of the Administration Server. The issuer name is used as an identifier of the Administration Server in the authenticator app. If you change the security code issuer name, you must issue a new secret key and pass it to the authenticator app. A security code is single-use and valid for up to 90 seconds (the exact time may vary).

Any user for whom two-step verification is enabled can reissue his or her own secret key. When a user authenticates with the reissued secret key and uses it for logging in, Administration Server saves the new secret key for the user account. If the user enters the new secret key incorrectly, Administration Server does not save the new secret key and leaves the current secret key valid for the further authentication.

Any authentication software that supports the Time-based One-time Password algorithm (TOTP) can be used as an authenticator app, for example, Google Authenticator. In order to generate the security code, you must synchronize the time set in the authenticator app with the time set for Administration Server.

To check if Kaspersky Security Center Linux supports the authenticator app that you want to use, enable two-step verification for all users or for a particular user.

One of the steps suggests that you specify the security code generated by the authenticator app. If it succeeds, then Kaspersky Security Center Linux supports the selected authenticator.

An authenticator app generates the security code as follows:

1. Administration Server generates a special secret key and QR code.
2. You pass the generated secret key or QR code to the authenticator app.
3. The authenticator app generates a single-use security code that you pass to the authentication window of Administration Server.

We highly recommend that you install an authenticator app on more than one device. Save the secret key (or QR code) and keep it in a safe place. This will help you to restore access to Kaspersky Security Center Web Console in case you lose access to your mobile device.

To secure the usage of Kaspersky Security Center Linux, you can enable two-step verification for your own account and enable two-step verification for all users.

You can [exclude](#) accounts from two-step verification. This can be necessary for service accounts that cannot receive a security code for authentication.

Two-step verification works according to the following rules:

- Only a user account that has the Modify object ACLs right in the **General features: User permissions** functional area can enable two-step verification for all users.
- Only a user that enabled two-step verification for his or her own account can enable the option of two-step verification for all users.
- Only a user that enabled two-step verification for his or her own account can exclude other user accounts from the list of two-step verification enabled for all users.
- A user can enable two-step verification only for his or her own account.
- A user account that has the Modify object ACLs right in the **General features: User permissions** functional area and is logged in to Kaspersky Security Center Web Console by using two-step verification can disable two-step verification: for any other user only if two-step verification for all users is disabled, for a user excluded from the list of two-step verification that is enabled for all users.
- Any user that logged in to Kaspersky Security Center Web Console by using two-step verification can reissue his or her own secret key.
- You can enable the two-step verification for all users option for the Administration Server you are currently working with. If you enable this option on the Administration Server, you also enable this option for the user accounts of its [virtual Administration Servers](#) and do not enable two-step verification for the user accounts of the secondary Administration Servers.

## Enabling two-step verification for your own account

You can enable two-step verification only for your own account.

Before you start enabling two-step verification for your account, ensure that an authenticator application is installed on your mobile device. Ensure that the time set in the authenticator application is synchronized with the time set of the device on which Administration Server is installed.

*To enable two-step verification for a user account:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the name of your account.
3. In the user settings window that opens, select the **Authentication security** tab:
  - a. Select the **Request user name, password, and security code (two-step verification)** option. Click the **Save** button.
  - b. In the two-step verification window that opens, click **View how to set up two-step verification**. Enter the secret key in the authenticator application or click **View QR code** and scan the QR code by the authenticator application on your mobile device to receive one-time security code.
  - c. In the two-step verification window, specify the security code generated by the authenticator application, and then click the **Check and apply** button.
4. Click the **Save** button.

Two-step verification is enabled for your account.

## Enabling two-step verification for all users

You can enable two-step verification for all users of Administration Server if your account has the Modify object ACLs right in the **General features: User permissions** functional area and if you are authenticated by using two-step verification.

*To enable two-step verification for all users:*

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 **Authentication security** tab of the properties window, switch the toggle button of the **two-step verification for all users** option to the enabled position.
3. If you did not [enable two-step verification for your account](#), the application opens the window for enabling two-step verification for your own account.
  - a. In the two-step verification window, click **View how to set up two-step verification**.
  - b. Enter the secret key in the authenticator application manually or click **View QR code** and scan the QR code by the authenticator application on your mobile device to receive one-time security code.
  - c. In the two-step verification window, specify the security code generated by the authenticator application, and then click the **Check and apply** button.

Two-step verification is enabled for all users. From now on, users of the Administration Server, including the users that were added after enabling two-step verification for all users, have to configure two-step verification for their accounts, except for users that are [excluded](#) from two-step verification.

## Disabling two-step verification for a user account

You can disable two-step verification for your own account, as well as for an account of any other user.

You can disable two-step verification of another user's account if your account has the Modify object ACLs right in the **General features: User permissions** functional area.

*To disable two-step verification for a user account:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the name of the internal user account for whom you want to disable two-step verification. This may be your own account or an account of any other user.
3. In the user settings window that opens, select the **Authentication security** tab.

4. Select the **Request only user name and password** option if you want to disable two-step verification for a user account.
5. Click the **Save** button.

Two-step verification is disabled for the user account.

## Disabling two-step verification for all users

You can disable two-step verification for all users if two-step verification is enabled for your account and your account has the Modify object ACLs right in the **General features: User permissions** functional area. If two-step verification is not enabled for your account, you must [enable two-step verification for your account](#) before disabling it for all users.

*To disable two-step verification for all users:*

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 **Authentication security** tab of the properties window, switch the toggle button of the **two-step verification for all users** option to disabled position.
3. Enter the credentials of your account in the authentication window.

Two-step verification is disabled for all users.

## Excluding accounts from two-step verification

You can exclude user accounts from two-step verification if you have the Modify object ACLs right in the **General features: User permissions** functional area.

If a user account is excluded from the list of two-step verification for all users, this user does not have to use two-step verification.

Excluding accounts from two-step verification can be necessary for service accounts that cannot pass the security code during authentication.

*If you want to exclude some user accounts from two-step verification:*

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 **Authentication security** tab of the properties window, in the two-step verification exclusions table click the **Add** button.
3. In the window that opens:
  - a. Select the user accounts that you want to exclude.



- b. Click the **OK** button.

The selected user accounts are excluded from two-step verification.

## Configuring two-step verification for your own account

The first time you sign in to Kaspersky Security Center Linux after two-step verification is enabled, the window for configuring two-step verification for your own account opens.

Before you configure two-step verification for your account, ensure that an authenticator application is installed on your mobile device. Ensure that the time on the device with the authenticator application and the time on the device with the Administration Server are synchronized to UTC, by using external time sources.

*To configure two-step verification for your account:*

1. Generate a one-time security code by using the authenticator application on your mobile device. To do this, perform one of the following actions:
  - Enter the secret key in the authenticator application manually.
  - Click **View QR code** and scan the QR code by using the authenticator application.

A security code will display on your mobile device.

2. In the configure two-step verification window, specify the security code generated by the authenticator application, and then click the **Check and apply** button.

Two-step verification is configured for your account. You are able to access the Administration Server in accordance with your rights.


## Prohibit new users from setting up two-step verification for themselves

In order to further improve Kaspersky Security Center Web Console 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-step verification, for example new domain administrator, cannot configure two-step verification for themselves. Therefore, such user cannot be authenticated on Administration Server and cannot sign in to Kaspersky Security Center Web Console without approval from another Kaspersky Security Center Linux administrator who already has two-step verification enabled.

This option is available if [two-step verification is enabled for all users](#).

*To prohibit new users from setting up two-step verification for themselves:*

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 **Authentication security** tab of the properties window, switch the toggle button **Prohibit new users from setting up two-step verification for themselves** to the enabled position.

This option does not affect the user accounts added to the [two-step verification exclusions](#).

In order to grant Kaspersky Security Center Web Console access to a user with disabled two-step verification, temporarily turn off the **Prohibit new users from setting up two-step verification for themselves** option, ask the user to enable two-step verification, and then turn on the option back.

## Generating a new secret key

You can generate a new secret key for a two-step verification for your account only if you are authorized by using two-step verification.

*To generate a new secret key for a user account:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the name of the user account for whom you want to generate a new secret key for two-step verification.
3. In the user settings window that opens, select the **Authentication security** tab.
4. On the **Authentication security** tab, click the **Generate a new secret key** link.
5. In the two-step verification window that opens, specify a new security key generated by the authenticator application.
6. Click the **Check and apply** button.

A new secret key is generated for the user.

If you lose your mobile device, you can install an authenticator application on another mobile device and generate a new secret key to restore access to Kaspersky Security Center Web Console.

## Editing the name of a security code issuer

You can have several identifiers (they are called issuers) for different Administration Servers. You can change the name of a security code issuer in case, for example, if the Administration Server already uses a similar name of security code issuer for another Administration Server. By default, the name of a security code issuer is the same as the name of the Administration Server.

After you change the security code issuer name you have to reissue a new secret key and pass it to the authenticator application.

*To specify a new name of security code issuer:*

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. In the user settings window that opens, select the **Authentication security** tab.
3. On the **Authentication security** tab, click the **Edit** link.  
The **Edit security code issuer** section opens.

4. Specify a new security code issuer name.
5. Click the **OK** button.

A new security code issuer name is specified for the Administration Server.

## Changing the number of allowed password entry attempts

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

By default, the maximum number of allowed attempts to enter a password is 10. You can change the number of allowed password entry attempts, as described in this section.

*To change the number of allowed password entry attempts:*

1. On the Administration Server device, run a Linux command line.
2. For the klscflag utility, run the following command:  

```
sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSp1PpcLogonAttempts -t d -v N
```

where N is a number of attempts to enter a password.
3. To apply the changes, restart the Administration Server service.

The maximum number of allowed password entry attempts is changed.

## Deleting a user or a security group

You can delete only internal users or internal security groups.

*To delete a user or a security group:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** or the **Groups** tab.
2. Select the check box next to the user or the security group that you want to delete.
3. Click **Delete**.
4. In the window that opens, click **OK**.

The user or the security group is deleted.

## Creating a user role

*To create a user role:*

1. In the main menu, go to **Users & roles** → **Roles**.
  2. Click **Add**.
  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 the 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 the changes.
- The updated role appears in the list of user roles.

## Editing the scope of a user role

A *user role scope* is a combination of users and administration groups. Settings associated with a user role apply only to devices that belong to users who have this role, and only if these devices belong to groups associated with this role, including child groups.

To add users, security groups, and administration groups to the scope of a user role, you can use either of the following methods:

*Method 1:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** or the **Groups** tab.
2. Select check boxes next to the users or security groups that you want to add to the user role scope.
3. Click the **Assign role** button.  
The Role assignment wizard starts. Proceed through the wizard by using the **Next** button.
4. On the **Select role** page of the wizard, select the user role that you want to assign.
5. On the **Define scope** page of the wizard, select the administration group that you want to add to the user role scope.
6. Click the **Assign role** button to close the window.

The selected users or security groups and the selected administration group are added to the scope of the user role.

*Method 2:*

1. In the main menu, go to **Users & roles** → **Roles**.
2. Click the name of the role for which you want to define the scope.
3. In the role properties window that opens, select the **Settings** tab.
4. In the **Role scope** section, click **Add**.  
The Role assignment wizard starts. Proceed through the wizard by using the **Next** button.
5. On the **Define scope** page of the wizard, select the administration group that you want to add to the user role scope.
6. On the **Select users** page of the wizard, select users and security groups that you want to add to the user role scope.
7. Click the **Assign role** button to close the window.
8. Click the **Close** button (✕) to close the role properties window.

The selected users or security groups and the selected administration group are added to the scope of the user role.

## 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. Click **Delete**.
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 & profiles** 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.

# API Reference Guide

This Kaspersky Security Center OpenAPI reference guide is designed to assist in the following tasks:

- Automation and customization. You can automate tasks that you might not want to handle manually. For example, as an administrator, you can use Kaspersky Security Center OpenAPI to create and run scripts that will facilitate developing the structure of administration groups and keep that structure up-to-date.
- Custom development. Using OpenAPI, you can develop a client application.

You can use the search field in the right part of the screen to locate the information you need in the OpenAPI reference guide.



## [OPENAPI REFERENCE GUIDE](#)

### Samples of scripts

The OpenAPI reference guide contains samples of the Python scripts listed in the table below. The samples show how you can call OpenAPI methods and automatically accomplish various tasks for protecting your network, for instance, create a ["primary/secondary" hierarchy](#), run [tasks](#) in Kaspersky Security Center Linux, or assign [distribution points](#). You can run the samples as is or create your own scripts based on the samples.

*To call the OpenAPI methods and run scripts:*

1. [Download the KIAkOAPI.tar.gz archive](#). This archive includes the KIAkOAPI package and samples (you can copy them from the archive or the OpenAPI reference guide). The KIAkOAPI.tar.gz archive is also located in the Kaspersky Security Center Linux installation folder.
2. [Install the KIAkOAPI package](#) from the KIAkOAPI.tar.gz archive on a device where Administration Server is installed.

You can call the OpenAPI methods, run the samples and your own scripts only on devices where Administration Server and the KIAkOAPI package are installed.

Matching between user scenarios and samples of Kaspersky Security Center OpenAPI methods

| Sample                                                                                   | Purpose of the sample                                                                                                                                                                                                                                             | Scenario                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Log KIAkParams</a>                                                           | You can extract and process data by using the KIAkParams data structure. The sample shows how to work with this data structure.<br><br>The sample output may be present in different ways. You can get the data to send an HTTP method or to use it in your code. | Monitoring and reporting                                                                                                                                                                       |
| <a href="#">Create and delete a "primary/secondary" hierarchy</a>                        | You can add a secondary Administration Server and establish a "primary/secondary" hierarchy. Alternately, you can disconnect the secondary Administration Server from the hierarchy.                                                                              | <a href="#">Creating a hierarchy of Administration Servers</a> , <a href="#">adding a secondary Administration Server</a> , and <a href="#">deleting a hierarchy of Administration Servers</a> |
| <a href="#">Download network list files via connection gateway to the specified host</a> | You can connect to Network Agent on the needed device by using a <a href="#">connection gateway</a> , and then download a file with the network list to your device.                                                                                              | <a href="#">Adjustment of distribution points and connection gateways</a>                                                                                                                      |
| <a href="#">Install a license key</a>                                                    | You can connect to the primary Administration                                                                                                                                                                                                                     | Licensing of managed                                                                                                                                                                           |

|                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                   |                                                                      |
|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| <a href="#">stored in the primary Administration Server repository onto the secondary Administration Servers</a> | <p>Server, download a required license key from it, and transmit this key to all the secondary Administration Servers included in a hierarchy.</p>                                                                                                                                                                                                                | <p>applications</p>                                                  |
| <a href="#">Create a report of effective user rights</a>                                                         | <p>You can create <a href="#">different reports</a>. For instance, you can generate the report of effective user rights by using this sample. This report describes the rights that a user has, depending on his or her group and role.</p> <p>You can download the report in the HTML, PDF, or Excel format.</p>                                                 | <p><a href="#">Generating and viewing a report</a></p>               |
| <a href="#">Start the device task</a>                                                                            | <p>You can connect to Network Agent on the needed device by using a <a href="#">connection gateway</a>, and then run the necessary task.</p>                                                                                                                                                                                                                      | <p><a href="#">Starting a task manually</a></p>                      |
| <a href="#">Register distribution points for devices in a group</a>                                              | <p>You can assign managed devices as distribution points (previously known as update agents).</p>                                                                                                                                                                                                                                                                 | <p><a href="#">Updating Kaspersky databases and applications</a></p> |
| <a href="#">Enumerate all groups</a>                                                                             | <p>You can perform various actions with administration groups. The sample shows how to do the following:</p> <ul style="list-style-type: none"> <li>• Get an identifier of the "Managed devices" root group</li> <li>• Move through the group hierarchy</li> <li>• Retrieve the full, expanded hierarchy of groups, along with their names and nesting</li> </ul> | <p><a href="#">Configuring Administration Server</a></p>             |
| <a href="#">Enumerate tasks, query task statistics, and run a task</a>                                           | <p>You can find out the following information:</p> <ul style="list-style-type: none"> <li>• Task progress history</li> <li>• Current task status</li> <li>• Number of tasks in different statuses</li> </ul> <p>You can also run a task. By default, the sample runs a task after it outputs statistics.</p>                                                      | <p>Monitoring task execution</p>                                     |
| <a href="#">Create and run a task</a>                                                                            | <p>You can create a task. Specify the following task parameters in the sample:</p> <ul style="list-style-type: none"> <li>• Type</li> <li>• Method of run</li> <li>• Name</li> <li>• Device group for which the task will be used</li> </ul>                                                                                                                      | <p>Creating a task</p>                                               |



|                                                  |                                                                                                                                                                                                                                                        |                                                                               |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
|                                                  | By default, the sample creates a task with the "Show message" type. You can run this task for all managed devices of Administration Server. If necessary, you can specify your own <a href="#">task parameters</a> .                                   |                                                                               |
| <a href="#">Enumerate license keys</a>           | You can get a list of all the active license keys for Kaspersky applications installed on managed devices of Administration Server. The list contains <a href="#">detailed data</a> about every license key, such as a name, type, or expiration date. | Viewing information about license keys in use                                 |
| <a href="#">Create and find an internal user</a> | You can create an account for further work.                                                                                                                                                                                                            | Selecting the account to start Administration Server                          |
| <a href="#">Create a custom category</a>         | You can create the application category with the needed <a href="#">parameters</a> .                                                                                                                                                                   | <a href="#">Creating an application category with content added manually.</a> |
| <a href="#">Enumerate users by using SrvView</a> | You can use the <a href="#">SrvView</a> class to request <a href="#">detailed information</a> from the Administration Server. For instance, you can get a list of users by using this sample.                                                          | Managing user accounts                                                        |

## Applications interacting with Kaspersky Security Center Linux via OpenAPI

Some applications interact with Kaspersky Security Center Linux via OpenAPI. Such applications include, for example, Kaspersky Anti Targeted Attack Platform or Kaspersky Security for Virtualization. This can also be a custom client application developed by you based on OpenAPI.

Applications interacting with Kaspersky Security Center Linux via OpenAPI connect to Administration Server. If you have configured an [allowlist of IP addresses](#) for connecting to the Administration Server, add IP addresses of devices where applications using Kaspersky Security Center Linux OpenAPI are installed. To find out whether the application that you use works by OpenAPI, see Help of this application.

# Updating Kaspersky databases and applications

This section describes steps you must take to regularly update the following:

- Kaspersky databases and software modules
- Installed Kaspersky applications, including Kaspersky Security Center Linux components and security applications

## Scenario: Regular updating Kaspersky databases and applications

This section provides a scenario for regular updating of Kaspersky databases, software modules, and applications. After you complete the [Configuring network protection scenario](#), you must maintain the reliability of the protection system to make sure that the Administration Servers and managed devices are kept protected against various threats, including viruses, network attacks, and phishing attacks.

Network protection is kept up-to-date by regular updates of the following:

- Kaspersky databases and software modules
- Installed Kaspersky applications, including Kaspersky Security Center Linux components and security applications

When you complete this scenario, you can be sure of the following:

- Your network is protected by the most recent Kaspersky software, including Kaspersky Security Center Linux components and security applications.
- The anti-virus databases and other Kaspersky databases critical for the network safety are always up-to-date.

## Prerequisites

The managed devices must have a connection to the Administration Server. If they do not have a connection, consider [updating Kaspersky databases and software modules manually](#) or [directly from the Kaspersky update servers](#).

Administration Server must have a connection to the internet.

Before you start, make sure that you have done the following:

1. Deployed the Kaspersky security applications to the managed devices according to the [scenario of deploying Kaspersky applications through Kaspersky Security Center Web Console](#).
2. Created and configured all required policies, policy profiles, and tasks according to the [scenario of configuring network protection](#).
3. [Assigned an appropriate amount of distribution points](#) in accordance with the number of managed devices and the network topology.

Updating Kaspersky databases and applications proceeds in stages:

### 1 Choosing an update scheme

There are [several schemes](#) that you can use to install updates for security applications. Choose the scheme or several schemes that meet the requirements of your network best.

## 2 Creating the task for downloading updates to the repository of the Administration Server

This task is created automatically by Kaspersky Security Center quick start wizard. If you did not run the wizard, create the task now.

This task is required to download updates from Kaspersky update servers to the repository of the Administration Server, as well as to update Kaspersky databases and software modules for Kaspersky Security Center Linux. After the updates are downloaded, they can be propagated to the managed devices.

If your network has assigned distribution points, the updates are automatically downloaded from the Administration Server repository to the repositories of the distribution points. In this case the managed devices included in the scope of a distribution point download the updates from the repository of the distribution point instead of the Administration Server repository.

How-to instructions: [Creating the task for downloading updates to the repository of the Administration Server](#)

## 3 Creating the task for downloading updates to the repositories of distribution points (optional)

By default, the updates are downloaded to the distribution points from the Administration server. You can configure Kaspersky Security Center Linux to download the updates to the distribution points directly from Kaspersky update servers. Download to the repositories of distribution points is preferable if the traffic between the Administration Server and the distribution points is more expensive than the traffic between the distribution points and Kaspersky update servers, or if your Administration Server does not have internet access.

When your network has assigned distribution points and the *Download updates to the repositories of distribution points* task is created, the distribution points download updates from Kaspersky update servers, and not from the Administration Server repository.

How-to instructions: [Creating the task for downloading updates to the repositories of distribution points](#)

## 4 Configuring distribution points

When your network has assigned distribution points, make sure that the **Deploy updates** option is enabled in the properties of all required distribution points. When this option is disabled for a distribution point, the devices included in the scope of the distribution point download updates from the repository of the Administration Server.

## 5 Optimizing the update process by using the diff files (optional)

You can optimize traffic between the Administration Server and the managed devices by using [diff files](#). When this feature is enabled, the Administration Server or a distribution point downloads diff files instead of entire files of Kaspersky databases or software modules. A diff file describes the differences between two versions of a file of a database or software module. Therefore, a diff file occupies less space than an entire file. This results in decrease in the traffic between the Administration Server or distribution points and the managed devices. To use this feature, enable the **Download diff files** option in the properties of the *Download updates to the Administration Server repository* task and/or the *Download updates to the repositories of distribution points* task.

How-to instructions: [Using diff files for updating Kaspersky databases and software modules](#)

## 6 Configuring automatic installation of updates for the security applications

Create the *Update* tasks for the managed applications to provide timely updates to the software modules and Kaspersky databases, including anti-virus databases. To ensure timely updates, we recommend that you select the **When new updates are downloaded to the repository** option when [configuring the task schedule](#).

If your network includes IPv6-only devices and you want to regularly update the security applications installed on these devices, make sure that the Administration Server version 13.2 and the Network Agent version 13.2 are installed on managed devices.

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.

## Results

Upon completion of the scenario, Kaspersky Security Center Linux is configured to update Kaspersky databases after the updates are downloaded to the repository of the Administration Server. You can then proceed to monitoring the network status.

## About updating Kaspersky databases, software modules, and applications

To be sure that the protection of your Administration Servers and managed devices is up-to-date, you must provide timely updates of the following:

- Kaspersky databases and software modules

Before downloading Kaspersky databases and software modules, Kaspersky Security Center Linux checks if Kaspersky servers are accessible. If access to the servers using system DNS is not possible, the application uses [public DNS servers](#). This is necessary to make sure anti-virus databases are updated and the level of security is maintained for the managed devices.

- Installed Kaspersky applications, including Kaspersky Security Center Linux components and security applications

Kaspersky Security Center Linux cannot update Kaspersky applications automatically. To update the applications, download the latest application versions from the Kaspersky website, and install them manually:

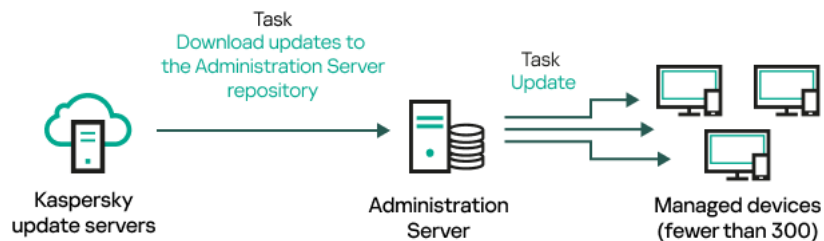
- [Kaspersky Security Center Linux Administration Server, Kaspersky Security Center Web Console](#) <sup>2</sup>
- [Network Agent, Kaspersky Endpoint Security, management web plug-in](#) <sup>2</sup>

Depending on the configuration of your network, you can use the following schemes of downloading and distributing the required updates to the managed devices:

- By using a single task: *Download updates to the Administration Server repository*
- By using two tasks:
  - The *Download updates to the Administration Server repository* task
  - The *Download updates to the repositories of distribution points* task
- Manually through a local folder, a shared folder, or an FTP server
- Directly from Kaspersky update servers to Kaspersky Endpoint Security on the managed devices
- Through a local or network folder if Administration Server has no internet connection

### Using the Download updates to the Administration Server repository task

In this scheme, Kaspersky Security Center Linux downloads updates through the *Download updates to the Administration Server repository* task. In small networks that contain less than 300 managed devices in a single network segment or less than 10 managed devices in each network segment, the updates are distributed to the managed devices directly from the Administration Server repository (see figure below).



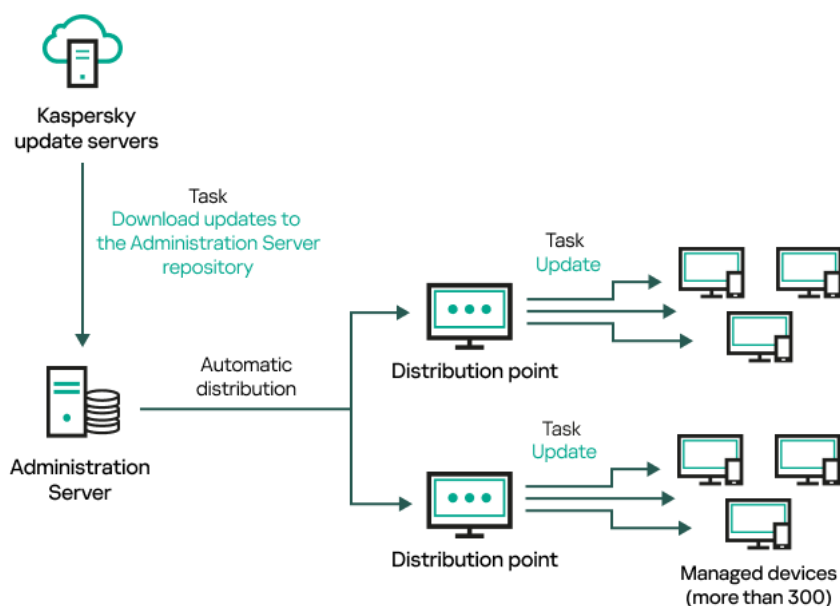
Updating by using the *Download updates to the Administration Server repository* task without distribution points

As a [source of updates](#), you can use not only Kaspersky update servers, but also a local or network folder.

By default, the Administration Server communicates with Kaspersky update servers and downloads updates by using the HTTPS protocol. You can configure the Administration Server to use the HTTP protocol instead of HTTPS.

If your network contains 300 managed devices or more in a single network segment or if your network consists of several network segments with more than 9 managed devices in each network segment, we recommend that you use [distribution points](#) to propagate the updates to the managed devices (see figure below). Distribution points reduce the load on the Administration Server and optimize traffic between the Administration Server and the managed devices. You can [calculate](#) the number and configuration of distribution points required for your network.

In this scheme, the updates are automatically downloaded from the Administration Server repository to the repositories of the distribution points. The managed devices included in the scope of a distribution point download the updates from the repository of the distribution point instead of the Administration Server repository.



Updating by using the *Download updates to the Administration Server repository* task with distribution points

When the *Download updates to the Administration Server repository* task is complete, the updates for Kaspersky databases and software modules for Kaspersky Endpoint Security are downloaded to the Administration Server repository. These updates are installed through the *Update* task for Kaspersky Endpoint Security.

The *Download updates to the repository of the Administration Server* task is not available on virtual Administration Servers. The repository of the virtual Administration Server displays updates downloaded to the primary Administration Server.

You can configure the updates to be verified for operability and errors on a set of test devices. If the verification is successful, the updates are distributed to other managed devices.

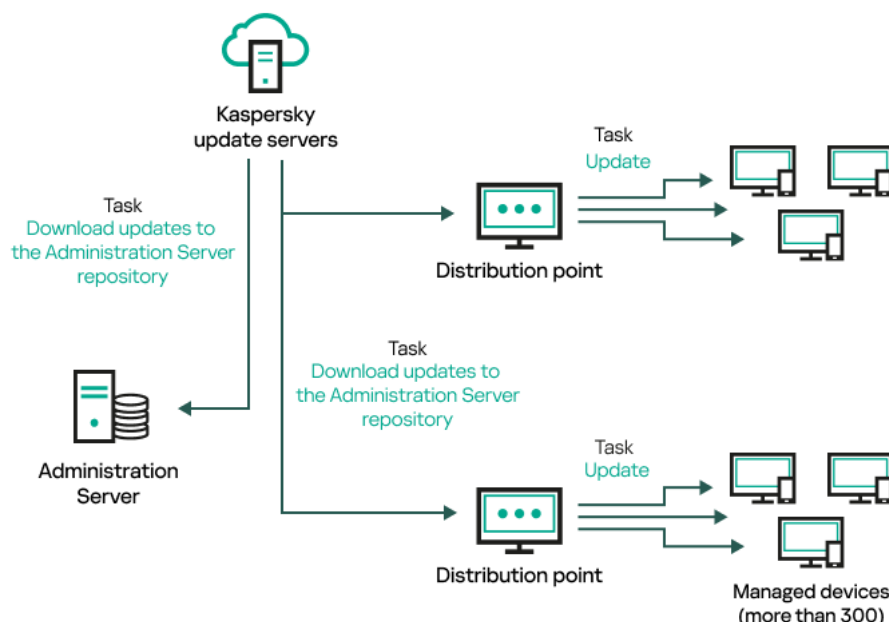
Each Kaspersky application requests required updates from Administration Server. Administration Server aggregates these requests and downloads only those updates that are requested by any application. This ensures that the same updates are not downloaded multiple times and that unnecessary updates are not downloaded at all. When running the *Download updates to the Administration Server repository* task, Administration Server sends the following information to Kaspersky update servers automatically in order to ensure the downloading of relevant versions of Kaspersky databases and software modules:

- Application ID and version
- Application setup ID
- Active key ID
- *Download updates to the repository of the Administration Server* task run ID

None of the transmitted information contains personal or other confidential data. AO Kaspersky Lab protects information in accordance with requirements established by law.

Using two tasks: the *Download updates to the Administration Server repository* task and the *Download updates to the repositories of distribution points* task

You can download updates to the repositories of distribution points directly from the Kaspersky update servers instead of the Administration Server repository, and then distribute the updates to the managed devices (see figure below). Download to the repositories of distribution points is preferable if the traffic between the Administration Server and the distribution points is more expensive than the traffic between the distribution points and Kaspersky update servers, or if your Administration Server does not have internet access.



Updating by using the *Download updates to the Administration Server repository* task and the *Download updates to the repositories of distribution points* task

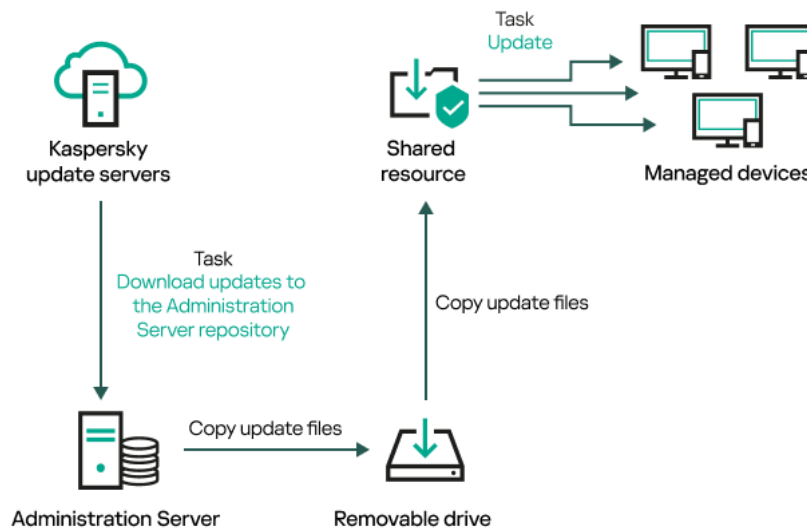
By default, the Administration Server and distribution points communicate with Kaspersky update servers and download updates by using the HTTPS protocol. You can configure the Administration Server and/or distribution points to use the HTTP protocol instead of HTTPS.

To implement this scheme, create the *Download updates to the repositories of distribution points* task in addition to the *Download updates to the Administration Server repository* task. After that the distribution points will download updates from Kaspersky update servers, and not from the Administration Server repository.

The *Download updates to the Administration Server repository* task is also required for this scheme, because this task is used to download Kaspersky databases and software modules for Kaspersky Security Center Linux.

## Manually through a local folder, a shared folder, or an FTP server

If the client devices do not have a connection to the Administration Server, you can use a local folder or a shared resource as a source for [updating Kaspersky databases, software modules, and applications](#). In this scheme, you need to copy required updates from the Administration Server repository to a removable drive, then copy the updates to the local folder or the shared resource specified as an update source in the settings of Kaspersky Endpoint Security (see figure below).



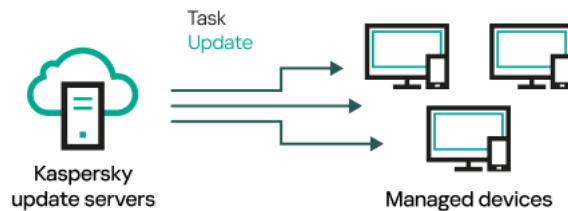
Updating through a local folder, a shared folder, or an FTP server

For more information about sources of updates in Kaspersky Endpoint Security, see the following Helps:

- [Kaspersky Endpoint Security for Linux Help](#)
- [Kaspersky Endpoint Security for Windows Help](#)

## Directly from Kaspersky update servers to Kaspersky Endpoint Security on the managed devices

On the managed devices, you can configure Kaspersky Endpoint Security to receive updates directly from Kaspersky update servers (see figure below).



Updating security applications directly from Kaspersky update servers

In this scheme, the security application does not use the repository provided by Kaspersky Security Center Linux. To receive updates directly from Kaspersky update servers, specify Kaspersky update servers as an update source in the security application. For more information about these settings, see the following Helps:

- [Kaspersky Endpoint Security for Linux Help](#)
- [Kaspersky Endpoint Security for Windows Help](#)

### Through a local or network folder if Administration Server has no internet connection

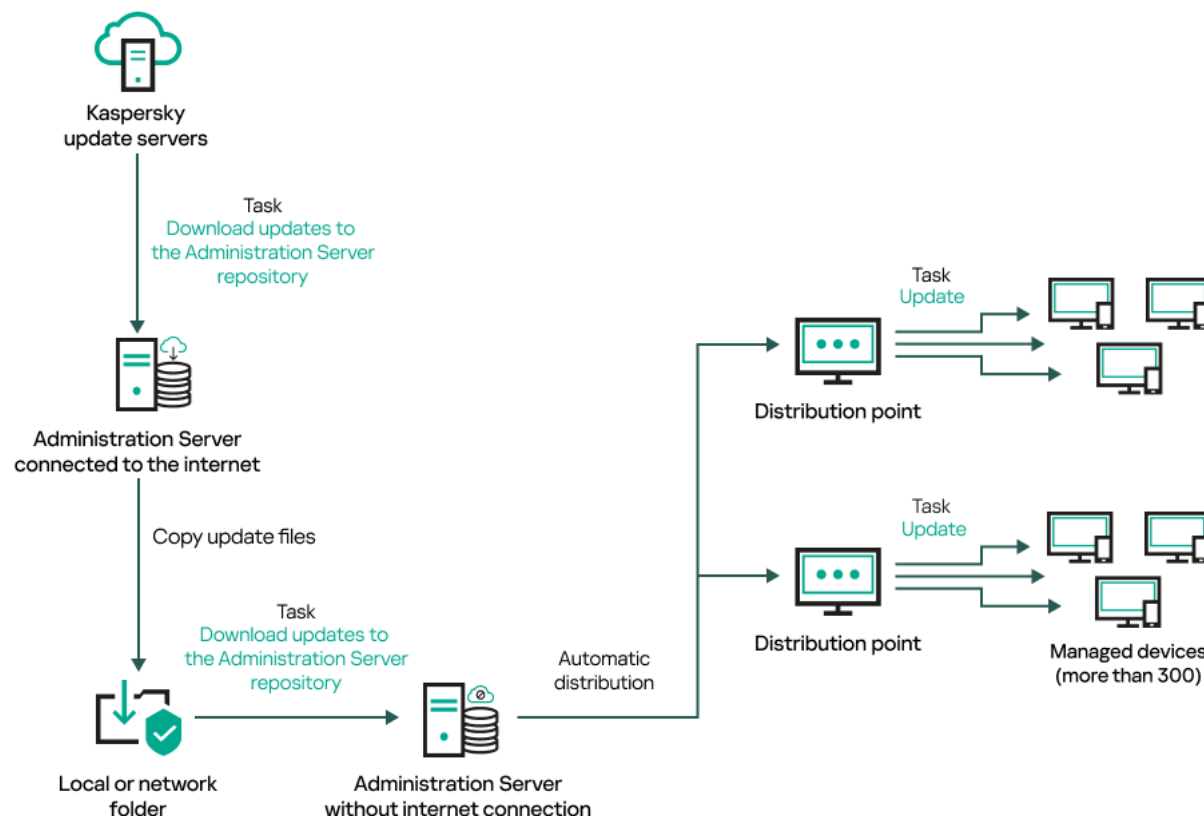
If Administration Server has no internet connection, you can configure the *Download updates to the Administration Server repository* task to download updates from a local or network folder. In this case, you must copy the required update files to the specified folder from time to time. For example, you can copy the required update files from one of the following sources:

- Administration Server that has an internet connection (see the figure below)

Because an Administration Server downloads only the updates that are requested by the security applications, the sets of security applications managed by the Administration Servers—the one that has an internet connection and the one that does not—must match.

If the Administration Server that you use to download updates has version 13.2 or earlier, open properties of the [Download updates to the Administration Server repository](#) task, and then enable the **Download updates by using the old scheme** option.





Updating through a local or network folder if Administration Server has no internet connection

- [Kaspersky Update Utility](#)

Because this utility uses the old scheme to download updates, open properties of the [Download updates to the Administration Server repository](#) task, and then enable the *Download updates by using the old scheme* option.

## Creating the Download updates to the Administration Server repository task

The *Download updates to the Administration Server repository* task allows you to download updates of databases and software modules for Kaspersky security applications from Kaspersky update servers to the Administration Server repository.

The Kaspersky Security Center quick start wizard [automatically creates](#) the *Download updates to the Administration Server repository* task of the Administration Server. In the task list, there can only be one *Download updates to the Administration Server repository* task. You can create this task again if it is removed from the task list of the Administration Server.

After the *Download updates to the Administration Server repository* task is complete and the updates are downloaded, they can be propagated to the managed devices.

Before you distribute updates to the managed devices, you can run the [Update verification](#) task. This allows you to make sure that Administration Server installs the downloaded updates properly and a security level is not decreased because of the updates. To verify them before distributing, configure the **Run update verification** option in the *Download updates to the Administration Server repository* task settings.

To create a *Download updates to the Administration Server repository* task:

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

2. Click **Add**.

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

3. For the Kaspersky Security Center application, select the **Download updates to the Administration Server repository** task type.

4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("\*<>?\\:|).

5. On the **Finish task creation** page, you can enable the **Open task details when creation is complete** option to open the task properties window and modify the default task settings. Otherwise, you can configure task settings later, at any time.

6. Click the **Finish** button.

The task is created and displayed in the task list.

7. Click the created task name to open the task properties window.

8. In the task properties window, on the **Application settings** tab, specify the following settings:

- **[Sources of updates](#)** 

As a [source of updates](#), you can use Kaspersky update servers, a local or network folder, or a primary Administration Server.

In the *Download updates to the Administration Server repository* task and the *Download updates to the repositories of distribution points* task, user authentication does not work if you select a password-protected local or network folder as an update source. To resolve this issue, first mount the password-protected folder, and then specify the required credentials, for example, by means of the operating system. After that, you can select this folder as an update source in an update download task. Kaspersky Security Center Linux will not require that you enter the credentials.

- **[Folder for storing updates](#)** 

The path to the [specified folder](#) for storing saved updates. You can copy the specified folder path to a clipboard. You cannot change the path to a specified folder for a group task.

- **[Force update of secondary Administration Servers](#)** 

If this option is enabled, the Administration Server starts the update tasks on the secondary Administration Servers as soon as new updates are downloaded. Otherwise, the update tasks on the secondary Administration Servers start according to their schedules.

By default, this option is disabled.

- **[Copy downloaded updates to additional folders](#)** 

After the Administration Server receives updates, it copies them to the specified folders. Use this option if you want to manually manage the distribution of updates on your network.

For example, you may want to use this option in the following situation: the network of your organization consists of several independent subnets, and devices from each of the subnets do not have access to other subnets. However devices in all of the subnets have access to a common network share. In this case, you set Administration Server in one of the subnets to download updates from Kaspersky update servers, enable this option, and then specify this network share. In downloaded updates to the repository tasks for other Administration Servers, specify the same network share as the update source.

By default, this option is disabled.

- [Download diff files](#) 

This option enables the [downloading diff files feature](#).

By default, this option is disabled.

- [Download updates by using the old scheme](#) 

Starting from version 14, Kaspersky Security Center Linux downloads updates of databases and software modules by using the new scheme. For the application to download updates by using the new scheme, the update source must contain the update files with the metadata compatible with the new scheme. If the update source contains the update files with the metadata compatible with the old scheme only, enable the **Download updates by using the old scheme** option. Otherwise, the update download task will fail.

For example, you must enable this option when a local or network folder is specified as an update source and the update files in this folder were downloaded by one of the following applications:

- [Kaspersky Update Utility](#) 

This utility downloads updates by using the old scheme.

- Kaspersky Security Center 13 Linux

For example, your Administration Server 1 does not have an internet connection. In this case, you may download updates by using an Administration Server 2 that has an internet connection, and then place the updates to a local or network folder to use it as an update source for the Administration Server 1. If the Administration Server 2 has version 13, enable the **Download updates by using the old scheme** option in the task for the Administration Server 1.

By default, this option is disabled.

- [Run update verification](#) 

Administration Server downloads updates from the source, saves them to a temporary repository, and [runs the task](#) defined in the **Update verification task** field. If the task completes successfully, the updates are copied from the temporary repository to a shared folder on the Administration Server and then distributed to all devices for which the Administration Server acts as the source of updates (tasks with the **When new updates are downloaded to the repository** schedule type are started). The task of downloading updates to the repository is finished only after completion of the *Update verification* task.

By default, this option is disabled.

9. In the task properties window, on the **Schedule** tab, create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

- **[Manually](#)** (selected by default)

The task does not run automatically. You can only start it manually.  
By default, this option is enabled.

- **[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 six 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 Security Center Linux.  
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 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.

- [Every month on specified days of selected weeks](#) 

The task runs regularly, on the specified days of each month, at the specified time.  
By default, no days of month are selected; the default start time is 6:00:00 PM.

- [On completing another task](#) 

The current task starts after another task completes. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. This parameter only works if both tasks are assigned to the same devices.

- Additional task settings:

- [Run missed tasks](#) 

This option determines the behavior of a task if a client device is not visible on the network when the task is about to start.

If this option is enabled, the system attempts to start the task the next time the Kaspersky application is run on the client device. If the task schedule is **Manually**, **Once** or **Immediately**, the task is started immediately after the device becomes visible on the network or immediately after the device is included in the task scope.

If this option is disabled, only scheduled tasks run on client devices; for **Manually**, **Once** and **Immediately**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- [Use automatically randomized delay for task starts](#) 

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However, when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- [Use randomized delay for task starts within an interval of \(min\)](#) <sup>?</sup>

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 \(min\)](#) <sup>?</sup>

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.

10. Click the **Save** button.

The task is created and configured.

When Administration Server performs the *Download updates to the Administration Server repository* task, updates to databases and software modules are downloaded from the updates source and stored in the shared folder of Administration Server. If you create this task for an administration group, it will only be applied to Network Agents included in the specified administration group.

Updates are distributed to client devices and secondary Administration Servers from the shared folder of Administration Server.

## Verifying downloaded updates

Before installing updates to the managed devices, you can first check the updates for operability and errors through the *Update verification* task. The *Update verification* task is performed automatically as part of the *Download updates to the Administration Server repository* task. The Administration Server downloads updates from the source, saves them in the temporary repository, and runs the *Update verification* task. If the task completes successfully, the updates are copied from the temporary repository to the Administration Server shared folder. They are distributed to all client devices for which the Administration Server is the source of updates.

If, as a result of the *Update verification* task, updates located in the temporary repository are incorrect or if the *Update verification* task completes with an error, such updates are not copied to the shared folder. The Administration Server retains the previous set of updates. Also, the tasks that have the **When new updates are downloaded to the repository** schedule type are not started then. These operations are performed at the next start of the *Download updates to the Administration Server repository* task if scanning of the new updates completes successfully.

A set of updates is considered invalid if any of the following conditions is met on at least one test device:

- An update task error occurred.
- The real-time protection status of the security application changed after the updates were applied.
- An infected object was detected during running of the on-demand scan task.

- A runtime error of a Kaspersky application occurred.

If none of the listed conditions is true for any test device, the set of updates is considered valid, and the *Update verification* task is considered to have completed successfully.

Before you start to create the *Update verification* task, perform the prerequisites:

1. [Create an administration group](#) with several test devices. You will need this group to verify the updates.

We recommend using devices with the most reliable protection and the most popular application configuration across the network. This approach increases the quality and probability of virus detection during scans, and minimizes the risk of false positives. If viruses are detected on test devices, the *Update verification* task is considered unsuccessful.

2. [Create the update and malware scan tasks](#) for an application supported by Kaspersky Security Center Linux, for example, Kaspersky Endpoint Security for Linux. When creating the update and malware scan tasks, specify the administration group with the test devices.

The *Update verification* task sequentially runs the update and malware scan tasks on test devices to check that all updates are valid. In addition, when creating the *Update verification* task, you need to specify the update and malware scan tasks.

3. Create the [Download updates to the Administration Server repository](#) task.

To make Kaspersky Security Center Linux verify downloaded updates before distributing them to client devices:

1. In the main menu, go to **Assets (Devices)** → **Tasks**.
2. Click the **Download updates to the Administration Server repository** task.
3. In the task properties window that opens, go to the **Application settings** tab, and then enable the **Run update verification** option.
4. If the *Update verification* task exists, click the **Select task** button. In the window that opens, select the *Update verification* task in the administration group with test devices.
5. If you did not create the *Update verification* task earlier, do the following:
  - a. Click the **New task** button.
  - b. In the New task wizard that opens, specify the task name if you want to change the preset name.
  - c. Select the administration group with test devices, which you created earlier.
  - d. First, select the update task of a required application supported by Kaspersky Security Center Linux, and then select the malware scan task.

After that, the following options appear. We recommend leaving them enabled:

- [Restart the device after database update](#) 

After anti-virus databases are updated on a device, we recommend rebooting the device.  
By default, the option is enabled.

- [Check real-time protection status after database update and device restart](#) 

If this option is enabled, the *Update verification* task checks whether updates downloaded to the Administration Server repository are valid, and if the protection level decreased after the anti-virus database update and device restart.

By default, this option is enabled.

e. Specify an account from which the *Update verification* task will be run. You can use your account and leave the **Default account** option enabled. Alternatively, you can specify that the task should be run under another account that has the necessary access rights. To do this, select the **Specify account** option, and then enter the credentials of that account.

6. Click **Save** to close the properties window of the *Download updates to the Administration Server repository* task.

The automatic update verification is enabled. Now, you can run the *Download updates to the Administration Server repository* task, and it will start from update verification.

## Creating the task for downloading updates to the repositories of distribution points

You can create the *Download updates to the repositories of distribution points* task for an administration group. This task will run for distribution points included in the specified administration group.

You can use this task, for example, if traffic between the Administration Server and the distribution point(s) is more expensive than traffic between the distribution point(s) and Kaspersky update servers, or if your Administration Server does not have internet access.

This task is required to download updates from Kaspersky update servers to the repositories of distribution points. The list of updates includes:

- Updates to databases and software modules for Kaspersky security applications
- Updates to Kaspersky Security Center components
- Updates to Kaspersky security applications

After the updates are downloaded, they can be propagated to the managed devices.

*To create the **Download updates to the repositories of distribution points** task, for a selected administration group:*

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

2. Click the **Add** button.

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

3. For the Kaspersky Security Center application, in the **Task type** field select **Download updates to the repositories of distribution points**.

4. Specify the name for the task that you are creating. A task name cannot be more than 100 characters long and cannot include any special characters ("\*<>?\\:|).



5. Select an option button to specify the administration group, the device selection, or the devices to which the task applies.
6. At the **Finish task creation** step, if you want to modify the default task settings, enable the **Open task details when creation is complete** option. If you do not enable this option, the task is created with the default settings. You can modify the default settings later, at any time.
7. Click the **Create** button.  
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(S) servers at Kaspersky from which Kaspersky applications download database and application module updates.

This option is selected by default.

- Primary Administration Server

This resource applies to tasks created for a secondary or virtual Administration Server.

- Local or network folder

A local or network folder that contains the latest updates. Only a mounted SMB share can be used as a network folder. When selecting a local folder, you must specify a folder on the device that has Administration Server installed.

In the *Download updates to the Administration Server repository* task and the *Download updates to the repositories of distribution points* task, user authentication does not work if you select a password-protected local or network folder as an update source. To resolve this issue, first mount the password-protected folder, and then specify the required credentials, for example, by means of the operating system. After that, you can select this folder as an update source in an update download task. Kaspersky Security Center Linux will not require that you enter the credentials.

- [Folder for storing updates](#) 

The path to the specified folder for storing saved updates. You can copy the specified folder path to a clipboard. You cannot change the path to a specified folder for a group task.

- [Download diff files](#) 

This option enables the [downloading diff files feature](#).

By default, this option is disabled.

- [Download updates by using the old scheme](#) 

Starting from version 14, Kaspersky Security Center Linux downloads updates of databases and software modules by using the new scheme. For the application to download updates by using the new scheme, the update source must contain the update files with the metadata compatible with the new scheme. If the update source contains the update files with the metadata compatible with the old scheme only, enable the **Download updates by using the old scheme** option. Otherwise, the update download task will fail.

For example, you must enable this option when a local or network folder is specified as an update source and the update files in this folder were downloaded by one of the following applications:

- [Kaspersky Update Utility](#)

This utility downloads updates by using the old scheme.

- Kaspersky Security Center 13 Linux

For example, a distribution point is configured to take the updates from a local or network folder. In this case, you may download updates by using an Administration Server that has an internet connection, and then place the updates to the local folder on the distribution point. If the Administration Server has version 13, enable the **Download updates by using the old scheme** option in the *Download updates to the repositories of distribution points* task.

By default, this option is disabled.

10. Create a schedule for task start. If necessary, specify the following settings:

- **Scheduled start:**

- [Manually](#) (selected by default)

The task does not run automatically. You can only start it manually.  
By default, this option is enabled.

- [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 six 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 \(daylight saving time is not supported\)](#) <sup>?</sup>

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 Security Center Linux.

By default, the task starts every day at the current system time.

- [Weekly](#) <sup>?</sup>

The task runs every week on the specified day and at the specified time.

- [By days of week](#) <sup>?</sup>

The task runs regularly, on the specified days of week, at the specified time.

By default, the task runs every Friday at 6:00:00 PM.

- [Monthly](#) <sup>?</sup>

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.

- [Every month on specified days of selected weeks](#) <sup>?</sup>

The task runs regularly, on the specified days of each month, at the specified time.

By default, no days of month are selected; the default start time is 6:00:00 PM.

- [On virus outbreak](#) <sup>?</sup>

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 anti-virus 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. You can select how the previous task must complete (successfully or with error) to trigger the start of the current task. This parameter only works if both tasks are assigned to the same devices.

- [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**, tasks run only on those client devices that are visible on the network. For example, you may want to disable this option for a resource-consuming task that you want to run only outside of business hours.

By default, this option is enabled.

- [Use automatically randomized delay for task starts](#) 

If this option is enabled, the task is started on client devices randomly within a specified time interval, that is, *distributed task start*. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

The distributed start time is calculated automatically when a task is created, depending on the number of client devices to which the task is assigned. Later, the task is always started on the calculated start time. However, when task settings are edited or the task is started manually, the calculated value of the task start time changes.

If this option is disabled, the task starts on client devices according to the schedule.

- [Use randomized delay for task starts within an interval of \(min\)](#) 

If this option is enabled, the task is started on client devices randomly within the specified time interval. A distributed task start helps to avoid a large number of simultaneous requests by client devices to the Administration Server when a scheduled task is running.

If this option is disabled, the task starts on client devices according to the schedule.

By default, this option is disabled. The default time interval is one minute.

11. Click the **Save** button.

The task is created and configured.

In addition to the settings that you specify during task creation, you can change other properties of a created task.

When the *Download updates to the repositories of distribution points* task is performed, updates for databases and software modules are downloaded from the update source and stored in the shared folder. Downloaded updates will only be used by distribution points that are included in the specified administration group and that have no update download task explicitly set for them.

## Adding sources of updates for the Download updates to the Administration Server repository task

When you create or use the [task for downloading updates to the Administration Server repository](#), you can choose the following sources of updates:

- Kaspersky update servers
- Primary Administration Server  
This resource applies to tasks created for a secondary or virtual Administration Server.
- Local or network folder

In the *Download updates to the Administration Server repository* task and the *Download updates to the repositories of distribution points* task, user authentication does not work if you select a password-protected local or network folder as an update source. To resolve this issue, first mount the password-protected folder, and then specify the required credentials, for example, by means of the operating system. After that, you can select this folder as an update source in an update download task. Kaspersky Security Center Linux will not require that you enter the credentials.

Kaspersky update servers are used by default, but you can also download updates from a local or network folder. You might want to use the folder if your network does not have access to the internet. In this case, you can manually download updates from Kaspersky update servers and put the downloaded files in the necessary folder.

You can specify only one path to a local or network folder. As a local folder, you must specify a folder on the device where Administration Server is installed. As a network folder, you can use an FTP or HTTP server or an SMB share. If an SMB share requires authentication, it must be mounted in the system with the required credentials in advance. We recommend not using the SMB1 protocol since it is insecure.

If you add both Kaspersky update servers and the local or network folder, updates will be downloaded first from the folder. In the case of an error when downloading, Kaspersky update servers will be used.

In case a shared folder that contains updates is password-protected, enable the **Specify account for access to shared folder of the update source (if any)** option and enter the account credentials required for access.

*To add the sources of updates:*

1. In the main menu, go to **Assets (Devices)** → **Tasks**.
2. Click **Download updates to the Administration Server repository**.
3. Go to the **Application settings** tab.
4. On the **Sources of updates** line, click the **Configure** button.
5. In the window that opens, click the **Add** button.
6. In the update source list, add the necessary sources. If you select the **Local or network folder** check box, specify a path to the folder.
7. Click **OK**, and then close the update source properties window.

8. In the update source window, click **OK**.

9. Click the **Save** button in the task window.

Now updates are downloaded to the Administration Server repository from the specified sources.

## About using diff files for updating Kaspersky databases and software modules

When Kaspersky Security Center Linux downloads updates from Kaspersky update servers, it optimizes traffic by using diff files. You can also enable the usage of diff files by devices (Administration Servers, distribution points, and client devices) that take updates from other devices on your network.

### About the Downloading diff files feature

A diff file describes the differences between two versions of a file of a database or software module. The usage of diff files saves traffic inside your company's network because diff files occupy less space than entire files of databases and software modules. If the *Downloading diff files* feature is enabled on Administration Server or a distribution point, the diff files are saved on this Administration Server or distribution point. As a result, devices that take updates from this Administration Server or distribution point can use the saved diff files to update their databases and software modules.

To optimize the usage of diff files, we recommend that you synchronize the update schedule of devices with the update schedule of the Administration Server or distribution point from which the devices take updates. However, the traffic can be saved even if devices are updated several times less often than are the Administration Server or distribution point from which the devices take updates.

Distribution points do not use IP multicasting for automatic distribution of diff files.

## Enabling the Downloading diff files feature: scenario

### Stages

#### 1 Enabling the feature on Administration Server

Enable the feature in the settings of a [Download updates to the repository of the Administration Server](#) task.

#### 2 Enabling the feature for a distribution point

Enable the feature for a distribution point that receives updates by means of a [Download updates to the repositories of distribution points](#) task.

Then enable the feature in the [Network Agent policy settings](#) for a distribution point that receives updates from Administration Server.

Then enable the feature for a distribution point that receives updates from Administration Server.

The feature is enabled in the [Network Agent policy settings](#) and—if the distribution points are assigned manually and if you want to override policy settings—in the [Distribution points](#) section of the Administration Server properties.

To check that the Downloading diff files feature is successfully enabled, you can measure the internal traffic before and after you perform the scenario.

## Downloading updates by distribution points

Kaspersky Security Center Linux allows distribution points to receive updates from the Administration Server, Kaspersky servers, or from a local or network folder.

*To configure update download for a distribution point:*

1. In the main menu, click the settings icon (⚙️) next to the name of the required Administration Server. The Administration Server properties window opens.
2. On the **General** tab, select the **Distribution points** section.
3. Click the name of the distribution point through which updates will be delivered to client devices in the group.
4. In the distribution point properties window, select the **Source of updates** section.
5. Select an update source for the distribution point:

- [Source of updates](#) ⓘ

Select a source of updates for the distribution point:

- To allow the distribution point to receive updates from the Administration Server, select **Retrieve from Administration Server**.
- To allow the distribution point to receive updates by using a task, select **Use update download task**, and then specify a *Download updates to the repositories of distribution points* task:
  - If such a task already exists on the device, select the task in the list.
  - If no such task yet exists on the device, click the **Create task** link to create a task. The New task wizard starts. Follow the instructions of the wizard.

- [Download diff files](#) ⓘ

This option enables the [downloading diff files feature](#).

By default, this option is enabled.

The distribution point will receive updates from the specified source.

## Updating Kaspersky databases and software modules on offline devices

Updating Kaspersky databases and software modules on managed devices is an important task for maintaining protection of the devices against viruses and other threats. Administrators usually configure [regular updates](#) through usage of the Administration Server repository.

When you need to update databases and software modules on a device (or a group of devices) that is not connected to the Administration Server (primary or secondary), a distribution point or the internet, you have to use alternative sources of updates, such as an FTP server or a local folder. In this case you have to deliver the files of the required updates by using a mass storage device, such as a flash drive or an external hard drive.

You can copy the required updates from:

- The Administration Server.  
To be sure the Administration Server repository contains the updates required for the security application installed on an offline device, at least one of the managed online devices must have the same security application installed. This application must be configured to receive the updates from the Administration Server repository through the *Download updates to the Administration Server repository* task.
- Any device that has the same security application installed and configured to receive the updates from the Administration Server repository, a distribution point repository, or directly from the Kaspersky update servers.

Below is an example of configuring updates of databases and software modules by copying them from the Administration Server repository.

*To update Kaspersky databases and software modules on offline devices:*

1. Connect the removable drive to the device where the Administration Server is installed.
2. Copy the updates files to the removable drive.

By default, the updates are located at: \\<server name>\KLSHARE\Updates.

Alternatively, you can configure Kaspersky Security Center Linux to regularly copy the updates to the folder that you select. For this purpose, use the **Copy downloaded updates to additional folders** option in the properties of the *Download updates to the Administration Server repository* task. If you specify a folder located on a flash drive or an external hard drive as a destination folder for this option, this mass storage device will always contain the latest version of the updates.

3. On offline devices, configure Kaspersky Endpoint Security to receive updates from a local folder or a shared resource, such as an FTP server or a shared folder.

How-to instructions:

- [Kaspersky Endpoint Security for Linux Help](#) 
- [Kaspersky Endpoint Security for Windows Help](#) 

4. Copy the updates files from the removable drive to the local folder or the shared resource that you want to use as an update source.
5. On the offline device that requires update installation, start the *Update* task of Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Windows, depending on the operating system of the offline device.

After the update task is complete, the Kaspersky databases and software modules are up-to-date on the device.

## Backing up and restoring web plug-ins



Kaspersky Security Center Web Console allows you to back up the current state of a web plug-in to be able to restore the saved state later. For example, you can back up a web plug-in before updating it to a newer version. After the update, if the newer version does not meet your requirements or expectations, you can restore the previous version of the web plug-in from the backup.

*To back up web plug-ins:*

1. In the main menu, go to **Settings** → **Web plug-ins**.
2. In the **Web plug-ins** section, select the web plug-ins that you want to back up, and then click the **Create backup copy** button.

The selected web plug-ins are backed up. You can view the created backups in the **Backups** section.

*To restore a web plug-in from a backup:*

1. In the main menu, go to **Settings** → **Backups**.
2. In the **Backups** section, select the backup of the web plug-in that you want to restore, and then click the **Restore from backup** button.

The web plug-in is restored from the selected backup.

# Monitoring, reporting, and audit

This section describes the monitoring and reporting capabilities of Kaspersky Security Center Linux. These capabilities give you an overview of your infrastructure, protection statuses, and statistics.

After Kaspersky Security Center Linux deployment or during the operation, you can configure the monitoring and reporting features to best suit your needs.

## Scenario: Monitoring and reporting

This section provides a scenario for configuring the monitoring and reporting feature in Kaspersky Security Center Linux.

### Prerequisites

After you deploy Kaspersky Security Center Linux in an organization's network you can start to monitor it and generate reports on its functioning.

Monitoring and reporting in an organization's network proceeds in stages:

#### 1 Configuring the switching of device statuses

Get acquainted with the settings for device statuses depending on specific conditions. By [changing these settings](#), you can change the number of events with *Critical* or *Warning* importance levels. When configuring the switching of device statuses, be sure of the following:

- New settings do not conflict with the information security policies of your organization.
- You are able to react to important security events in your organization's network in a timely manner.

#### 2 Configuring notifications about events on client devices

How-to instructions:

[Configure notification \(by email, by SMS, or by running an executable file\) of events on client devices](#)

#### 3 Performing recommended actions for Critical and Warning notifications

How-to instructions:

[Perform recommended actions for your organization's network](#)

#### 4 Reviewing the security status of your organization's network

How-to instructions:

- [Review the Protection status widget](#)
- [Generate and review the Report on protection status](#)
- [Generate and review the Report on errors](#)

#### 5 Locating client devices that are not protected

How-to instructions:

- [Review the New devices widget](#)

- [Generate and review the Report on protection deployment](#)

## 6 Checking protection of client devices

How-to instructions:

- [Generate and review reports from the Protection status and Threat statistics categories](#)
- [Start and review the Critical event selection](#)

## 7 Evaluating and limiting the event load on the database

Information about events that occur during operation of managed applications is transferred from a client device and registered in the Administration Server database. To reduce the load on the Administration Server, evaluate and limit the maximum number of events that can be stored in the database.

How-to instructions:

- [Limiting the maximum number of events](#)

## 8 Reviewing license information

How-to instructions:

- [Add the License key usage widget to the dashboard and review it](#)
- [Generate and review the Report on usage of license keys](#)

## Results

Upon completion of the scenario, you are informed about protection of your organization's network and, thus, can plan actions for further protection.

## About types of monitoring and reporting

Information on security events in an organization's network is stored in the Administration Server database. Based on the events, Kaspersky Security Center Web Console provides the following types of monitoring and reporting in your organization's network:

- Dashboard
- Reports
- Event selections
- Notifications

### Dashboard

The dashboard allows you to monitor security trends on your organization's network by providing you with a graphical display of information.

### Reports

The Reports feature allows you to get detailed numerical information about the security of your organization's network, save this information to a file, send it by email, and print it.

## Event selections

Event selections provide an onscreen view of named sets of events that are selected from the Administration Server database. These sets of events are grouped according to the following categories:

- By importance level—**Critical events**, **Functional failures**, **Warnings**, and **Info events**
- By time—**Recent events**
- By type—**User requests** and **Audit events**

You can create and view user-defined event selections based on the settings available, in the Kaspersky Security Center Web Console interface, for configuration.

## Notifications

Notifications alert you about events and help you to speed up your responses to these events by performing recommended actions or actions you consider as appropriate.

## Dashboard and widgets

This section contains information about the dashboard and the widgets that the dashboard provides. The section includes instructions on how to manage widgets and configure widget settings.

## Using the dashboard

The dashboard allows you to monitor security trends on your organization's network by providing you with a graphical display of information.

The dashboard is available in the Kaspersky Security Center Web Console, in the **Monitoring & reporting** section, by clicking **Dashboard**.

The dashboard provides widgets that can be customized. You can choose a large number of different widgets, presented as pie charts or donut charts, tables, graphs, bar charts, and lists. The information displayed in widgets is automatically updated, the update period is one to two minutes. The interval between updates varies for different widgets. You can refresh data on a widget manually at any time by means of the settings menu.

By default, widgets include information about all events stored in the database of Administration Server.

Kaspersky Security Center Web Console has a default set of widgets for the following categories:

- **Protection status**
- **Deployment**
- **Updating**

- **Threat statistics**
- **Other**

Some widgets have text information with links. You can view detailed information by clicking a 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 & reporting** → **Dashboard**.
2. Click the **Add or restore web 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 the **Add** button.

The selected widgets are added at the end of the dashboard.

You can now edit the [representation](#) and [parameters](#) of the added widgets.

## Hiding a widget from the dashboard

*To hide a displayed widget from the dashboard:*

1. In the main menu, go to **Monitoring & reporting** → **Dashboard**.
2. Click the settings icon (⚙️) next to the widget that you want to hide.
3. Select **Hide web 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 & reporting** → **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 & reporting** → **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 & reporting** → **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 the 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:

- **Web widget scope** (the set of objects for which the widget displays information)—for example, an administration group or device selection.
- **Select task** (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.
- **Set to Critical if these are specified** and **Set to Warning if these are specified** (the rules that determine the color of a traffic light).

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 & reporting** → **Dashboard**.
2. Click the settings icon (⚙️) next to the widget that you want to move.
3. Select **Refresh**.

The data on the widget is refreshed.

## About the Dashboard-only mode

You can [configure the Dashboard-only mode](#) for employees who do not manage the network but who want to view the network protection statistics in Kaspersky Security Center Linux (for example, a top manager). When a user has this mode enabled, only a dashboard with a predefined set of widgets is displayed to the user. Thus, he or she can monitor the statistics specified in the widgets, for example, the protection status of all managed devices, the number of recently detected threats, or the list of the most frequent threats in the network.

When a user works in the Dashboard-only mode, the following restrictions are applied:

- The main menu is not displayed to the user, so he or she cannot change the network protection settings.
- The user cannot perform any actions with widgets, for example, add or hide them. Therefore, you need to put all widgets required for the user on the dashboard and configure them, for instance, set the rule of counting objects or specify the time interval.

You cannot assign the Dashboard-only mode to yourself. If you want to work in this mode, contact a system administrator, Managed Service Provider (MSP), or a user with the [Modify object ACLs](#) right in the **General features: User permissions** functional area.

## Configuring the Dashboard-only mode

Before you begin to configure the [Dashboard-only mode](#), make sure that the following prerequisites are met:

- You have the [Modify object ACLs](#) right in the **General features: User permissions** functional area. If you do not have this right, the tab for configuring the mode will be missing.
- The user has the [Read](#) right in the **General features: Basic functionality** functional area.

If a hierarchy of Administration Servers is arranged in your network, for configuring the Dashboard-only mode go to the Server where the user account is available on the **Users** tab of the **Users & roles** → **Users & groups** section. It can be a primary server or physical secondary server. It is not possible to adjust the mode on a virtual server.

*To configure the Dashboard-only mode:*

1. In the main menu, go to **Users & roles** → **Users & groups**, and then select the **Users** tab.
2. Click the user account name for which you want to adjust the dashboard with widgets.
3. In the account settings window that opens, select the **Dashboard** tab.  
On the tab that opens, the same dashboard is displayed for you as for the user.
4. If the **Display the console in Dashboard-only mode** option is enabled, switch the toggle button to disable it.  
When this option is enabled, you are also unable to change the dashboard. After you disable the option, you can manage widgets.
5. Configure the dashboard appearance. The set of widgets prepared on the **Dashboard** tab is available for the user with the customizable account. He or she cannot change any settings or size of the widgets, add, or remove any widgets from the dashboard. Therefore, adjust them for the user, so he or she can view the network protection statistics. For this purpose, on the **Dashboard** tab you can perform the same actions with widgets as in the **Monitoring & reporting** → **Dashboard** section:
  - [Add new widgets](#) to the dashboard.
  - [Hide widgets](#) that the user doesn't need.
  - [Move widgets](#) into a specific order.
  - [Change the size or appearance](#) of widgets.
  - [Change the widget settings](#).
6. Switch the toggle button to enable the **Display the console in Dashboard-only mode** option.  
After that, only the dashboard is available for the user. He or she can monitor statistics but cannot change the network protection settings and dashboard appearance. As the same dashboard is displayed for you as for the user, you are also unable to change the dashboard.  
If you keep the option disabled, the main menu is displayed for the user, so he or she can perform various actions in Kaspersky Security Center Linux, including changing security settings and widgets.



7. Click the **Save** button when you finish configuring the Dashboard-only mode. Only after that will the prepared dashboard be displayed to the user.
8. If the user wants to view statistics of supported Kaspersky applications and needs access rights to do so, [configure the rights](#) for the user. After that, Kaspersky applications data is displayed for the user in the widgets of these applications.

Now the user can log in to Kaspersky Security Center Linux under the customized account and monitor the network protection statistics in the Dashboard-only mode.

## Reports

This section describes how to use reports, manage custom report templates, use report templates to generate new reports, and create report delivery tasks.

## Using reports

The Reports feature allows you to get detailed numerical information about the security of your organization's network, save this information to a file, send it by email, and print it.

Reports are available in the Kaspersky Security Center Web Console, in the **Monitoring & reporting** section, by clicking **Reports**.

By default, reports include information for the last 30 days.

Kaspersky Security Center Linux has a default set of reports for the following categories:

- **Protection status**
- **Deployment**
- **Updating**
- **Threat statistics**
- **Other**

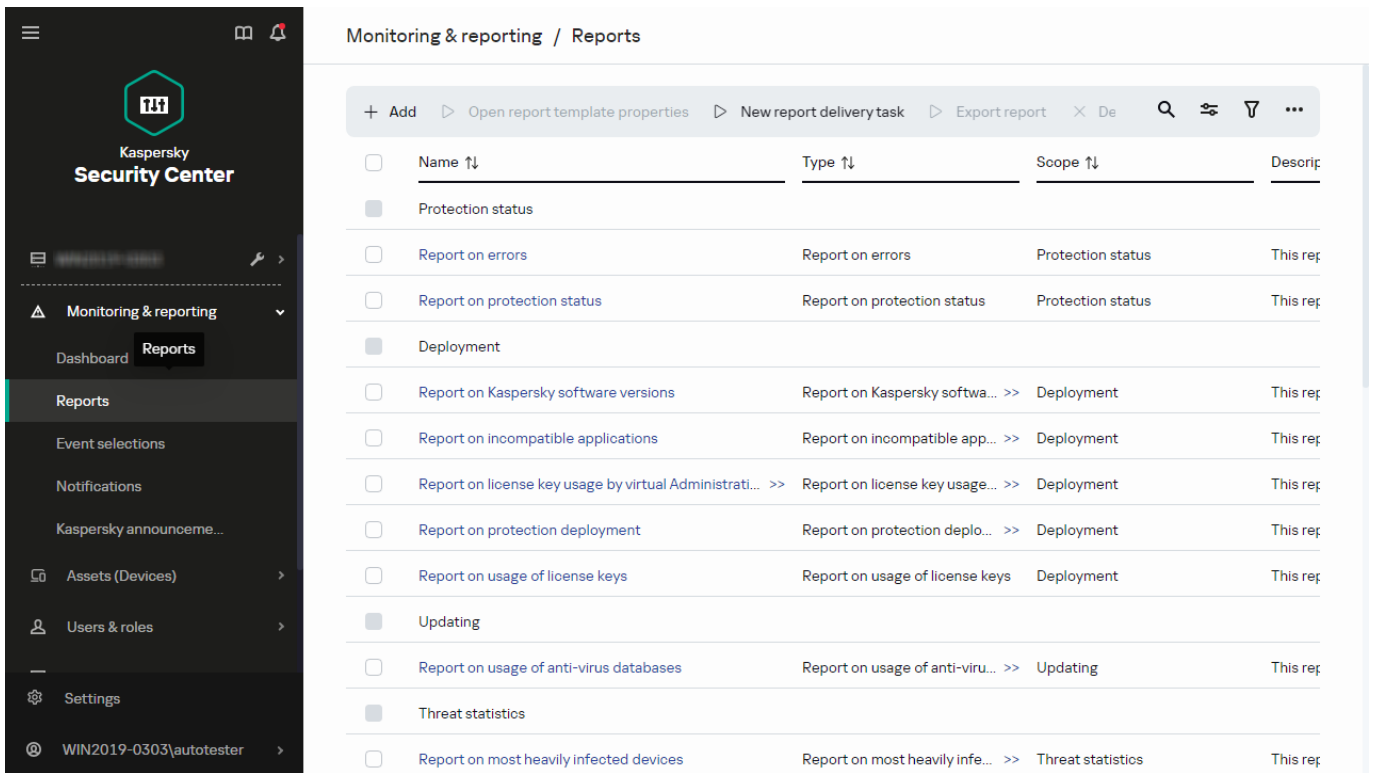
You can [create custom report templates](#), [edit report templates](#), and [delete them](#).

You can [create reports](#) that are based on existing templates, [export reports to files](#), and [create tasks for report delivery](#).

## Creating a report template

*To create a report template:*

1. In the main menu, go to **Monitoring & reporting** → **Reports**.

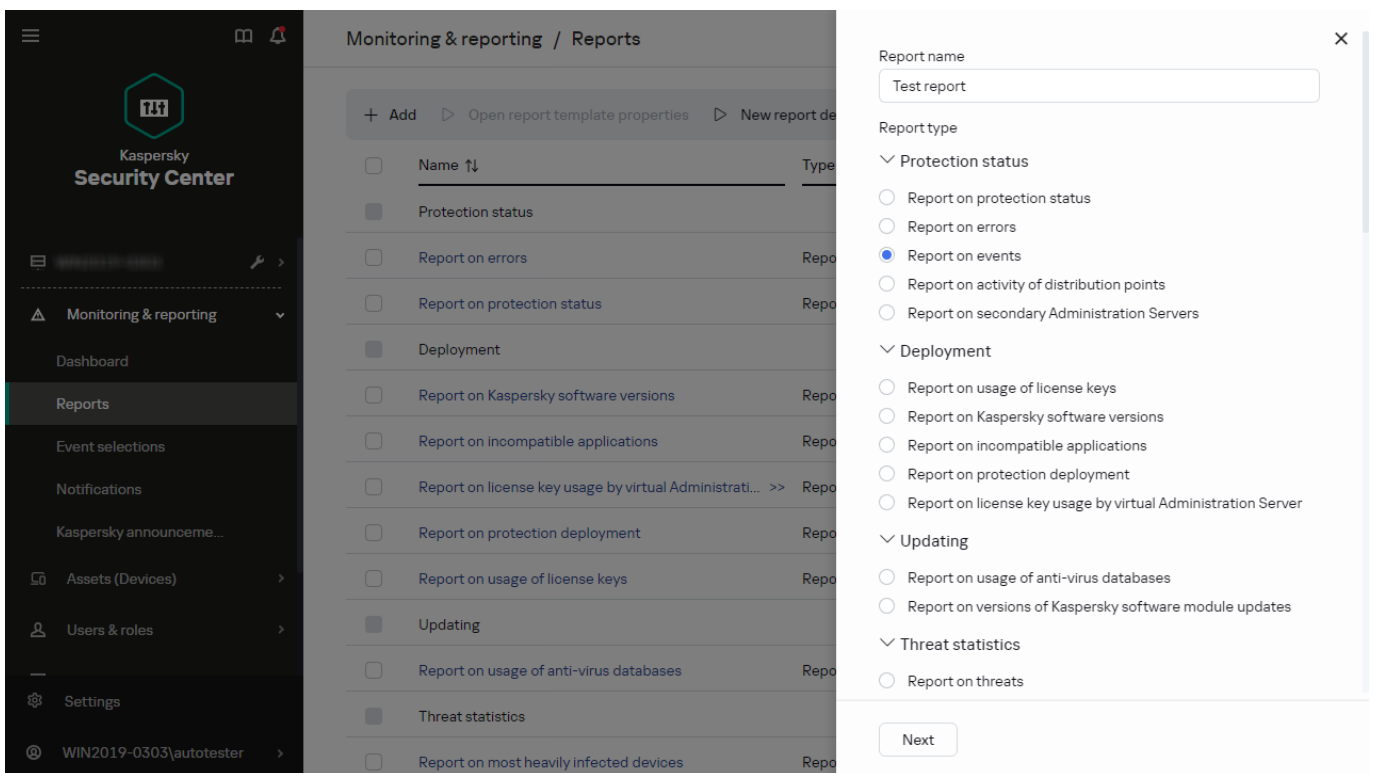


The list of the report templates in the Reports subsection

2. Click **Add**.

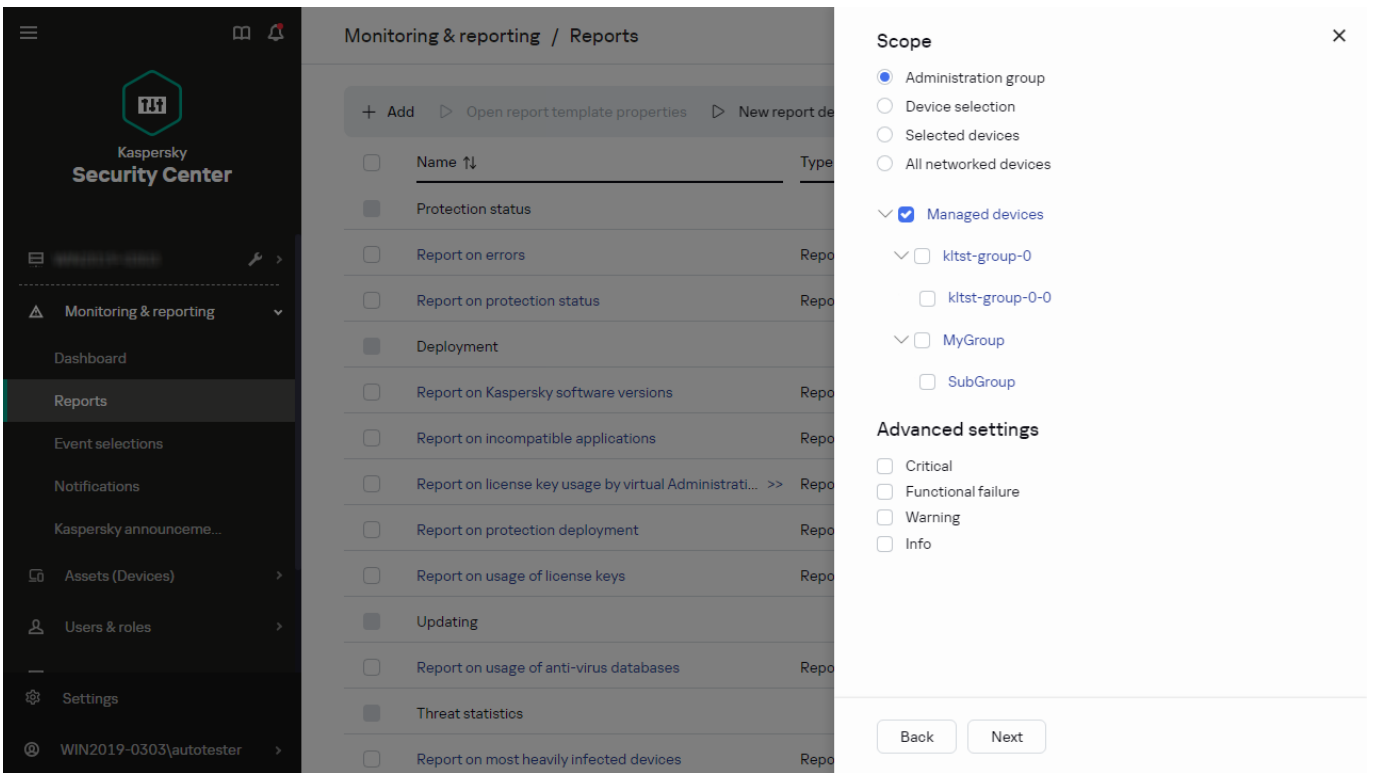
The New report template wizard starts. Proceed through the wizard by using the **Next** button.

3. On the first page of the wizard, enter the report name and select the report type.



The New report template wizard. Specifying the name and type of the report template

4. On the **Scope** page 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.

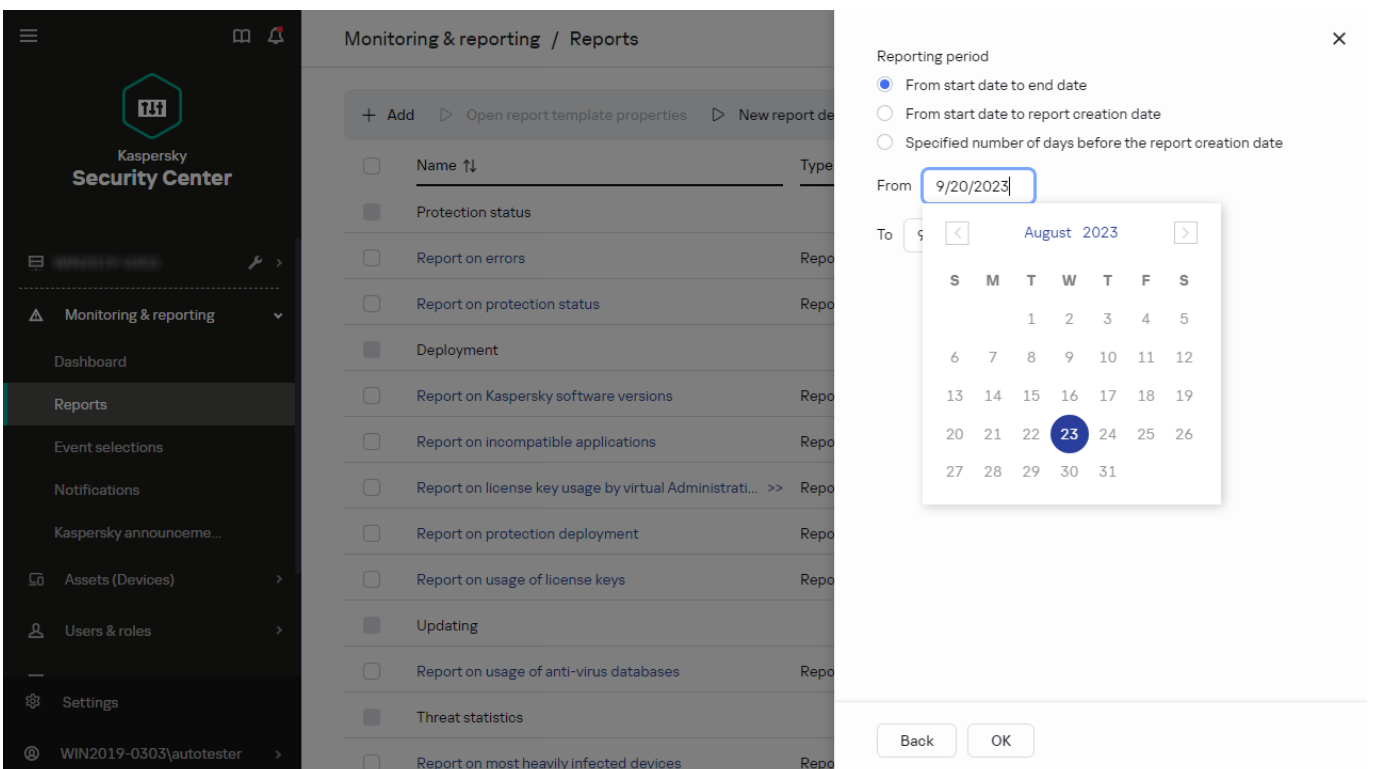


The New report template wizard. Specifying the report template scope

5. On the **Reporting period** page of the wizard, specify the report period. Available values are as follows:

- 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.



The New report template wizard. Specifying the reporting period

6. Click **OK** to close the wizard.

7. Do one of the following:

- Click the **Save and run** button to save the new report template and to run a report based on it.  
The report template is saved. The report is generated.
- Click the **Save** button to save the new report template.  
The report template is saved.


You can use the new template for generating and viewing reports.

## 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 & reporting** → **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, your device may run out of memory while generating such a report and, consequently, you will not be able to view the report.

By default, this option is enabled. The default value is 1000.

- **Group**

Click the **Settings** button to change the set of client devices for which the report is created. For some types of the reports, the button may be unavailable. The actual settings depend on the settings specified during creation of the report template.

- **Time interval**

Click the **Settings** button to modify the report period. For some types of the reports, the button may be unavailable. Available values are as follows:

- 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, this 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 at regular intervals 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 will be displayed in the report, and use the **Move up** button and **Move down** button to change the order of these fields. Use the **Add** button or **Edit** button to specify whether the information in the report must be sorted and filtered by each of the fields.

In the **Filters of Details fields** section, you can also click the **Convert filters** button to start using the extended filtering format. This format enables you to combine filtering conditions specified in various fields by using the logical OR operation. After you click the button, the **Convert filters** panel opens on the right. Click the **Convert filters** button to confirm conversion. You can now define a converted filter with conditions from the **Details fields** section that are applied by using the logical OR operation.

Conversion of a report to the format supporting complex filtering conditions will make the report incompatible with the previous versions of Kaspersky Security Center (11 and earlier). Also, the converted report will not contain any data from secondary Administration Servers running such incompatible versions.

5. Click **Save** to save the changes.

6. Close the **Editing report <Report name>** window.

The updated report template appears in the list of report templates.

## Exporting a report to a file

You can save one or multiple reports as XML, HTML, or PDF. Kaspersky Security Center Linux allows you to export up to 10 reports to files of the specified format at the same time.

*To export a report to a file:*

1. In the main menu, go to **Monitoring & reporting** → **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 window that opens, specify the following export parameters:

- **File name.**

If you select one report to export, specify the report file name.

If you select more than one report, the report file names will coincide with the name of the selected report templates.

- **Maximum number of entries.**

Specify the maximum number of entries included in the report file. The default value is 10,000.

You can export a report with an unlimited number of entries. Note that if your report contains a large number of entries, the time required for generating and exporting the report increases.

- **File format.**

Select the report file format: XML, HTML, or PDF. If you export multiple reports, all selected reports are saved in the specified format as separate files.

The wkhtmltopdf tool is required to convert a report to PDF. When you select the PDF option, Administration Server checks whether the wkhtmltopdf tool is installed on the device. If the tool is not installed, the application displays a message about the necessity to install the tool on the Administration Server device. Install the tool manually, and then proceed to the next step.

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 & reporting** → **Reports**.

2. Click the name of the report template that you want to use to create a report.

A report using the selected template is generated and displayed.

Report data is displayed according to the localization set for the Administration Server.

In the generated reports, some fonts may be displayed incorrectly on the diagrams. To resolve this issue, install the fontconfig library. Also, please check that the fonts corresponding to your operating system locale are installed in the operating system.

The report displays the following data:

- On the **Summary** tab:

- The name and type of report, a brief description and the reporting period, as well as information about the group of devices for which the report is generated.
- Graph chart showing the most representative report data.
- Consolidated table with calculated report indicators.
- On the **Details** tab, a table with detailed report data is displayed.

## Creating a report delivery task

You can create a task that will deliver selected reports.

*To create a report delivery task:*

1. In the main menu, go to **Monitoring & reporting** → **Reports**.
2. [Optional] Select the check boxes next to the report templates for which you want to create a report delivery task.
3. Click the **New report delivery task** button.
4. The New task wizard starts. Proceed through the wizard by using the **Next** button.
5. On the first page of the wizard, enter the task name. The default name is **Deliver reports (<N>)**, where <N> is the sequence number of the task.
6. On the task settings page of the wizard, specify the following settings:
  - a. Report templates to be delivered by the task. If you selected them at step 2, skip this step.
  - 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.
  - d. Whether the reports are to be saved to a folder, whether previously saved reports in this folder are to be overwritten, and whether a specific account is to be used to access the folder (for a shared folder).
7. If you want to modify other task settings after the task is created, on the **Finish task creation** page of the wizard enable the **Open task details when creation is complete** option.
8. Click the **Create** button to create the task and close the wizard.  
 The report delivery task is created. If you enabled the **Open task details when creation is complete** option, the task settings window opens.

## Deleting report templates



To delete one or several report templates:

1. In the main menu, go to **Monitoring & reporting** → **Reports**.
2. Select check boxes next to the report templates that you want to delete.
3. 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 Security Center Linux components, and about managing frequent events blocking.

## About events in Kaspersky Security Center Linux

Kaspersky Security Center Linux allows you to receive information about events that occur during the operation of Administration Server and Kaspersky applications installed on managed devices. Information about events is saved in the Administration Server database.

### Events by type

In Kaspersky Security Center Linux, there are the following types of events:

- General events. These events occur in all managed Kaspersky applications. An example of a general event is Virus outbreak. General events have strictly defined syntax and semantics. General events are used, for instance, in reports and dashboards.
- Managed Kaspersky applications-specific events. Each managed Kaspersky application has its own set of events.

### Events by source

You can view the full list of the events that can be generated by an application on the **Event configuration** tab in the application policy. For Administration Server, you can additionally view the event list in the Administration Server properties.

Events can be generated by the following applications:

- Kaspersky Security Center Linux components:
  - [Administration Server](#)
  - [Network Agent](#)

- Managed Kaspersky applications

For details about the events generated by Kaspersky managed applications, please refer to the documentation of the corresponding application.

## Events by importance level

Each event has its own importance level. Depending on the conditions of its occurrence, an event can be assigned various importance levels. There are four importance levels of events:

- A *critical event* is an event that indicates the occurrence of a critical problem that may lead to data loss, an operational malfunction, or a critical error.
- A *functional failure* is an event that indicates the occurrence of a serious problem, error or malfunction that occurred during operation of the application or while performing a procedure.
- A *warning* is an event that is not necessarily serious, but nevertheless indicates a potential problem in the future. Most events are designated as warnings if the application can be restored without loss of data or functional capabilities after such events occur.
- An *info* event is an event that occurs for the purpose of informing about successful completion of an operation, proper functioning of the application, or completion of a procedure.

Each event has a defined storage term, during which you can view or modify it in Kaspersky Security Center Linux. Some events are not saved in the Administration Server database by default because their defined storage term is zero. Only events that will be stored in the Administration Server database for at least one day can be exported to external systems.

## Events of Kaspersky Security Center Linux components

Each Kaspersky Security Center Linux component has its own set of event types. This section lists types of events that occur in Kaspersky Security Center Administration Server and Network Agent. Types of events that occur in Kaspersky applications are not listed in this section.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. For Administration Server, you can additionally view and configure the event list in the Administration Server properties. If you want to configure notification settings for all the events at once, [configure general notification settings](#) in the Administration Server properties.

## Data structure of event type description

For each event type, its display name, identifier (ID), alphabetic code, description, and the default storage term are provided.

- **Event type display name.** This text is displayed in Kaspersky Security Center Linux when you configure events and when they occur.
- **Event type ID.** This numerical code is used when you process events by using third-party tools for event analysis.

- **Event type** (alphabetic code). This code is used when you browse and process events by using public views that are provided in the Kaspersky Security Center Linux database and when events are exported to a SIEM system.
- **Description**. This text contains the situations when an event occurs and what you can do in such a case.
- **Default storage term**. This is the number of days during which the event is stored in the Administration Server database and is displayed in the list of events on Administration Server. After this period elapses, the event is deleted. If the event storage term value is 0, such events are detected but are not displayed in the list of events on Administration Server. If you configured to save such events to the operating system event log, you can find them there.

You can change the storage term for events: [Setting the storage term for an event](#)

## Administration Server events

This section contains information about the events related to the Administration Server.

### Administration Server critical events

The table below shows the events of Kaspersky Security Center 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.

Administration Server critical events

| 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 | <p>Once a day Kaspersky Security Center Linux checks whether a licensing restriction is exceeded.</p> <p>Events of this type occur when Administration Server detects that some licensing limits are exceeded by Kaspersky applications installed on client devices and if the number of currently used <a href="#">licensing units</a> covered by a single license exceeds 110% of the total number of units covered by the license.</p> <p>Even when this event occurs, client devices are protected.</p> <p>You can respond to the event in the following ways:</p> | 180 days             |

|                                             |      |                                  |                                                                                                                                                                                                                                                                                                                                                                                             |          |
|---------------------------------------------|------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                             |      |                                  | <ul style="list-style-type: none"> <li>• Look through the managed devices list. Delete devices that are not in use.</li> <li>• Provide a license for more devices (add a valid activation code or a key file to Administration Server).</li> </ul> <p>Kaspersky Security Center Linux determines <a href="#">the rules to generate events</a> when a licensing restriction is exceeded.</p> |          |
| Device has become unmanaged                 | 4111 | KLSRV_HOST_OUT_CONTROL           | <p>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 of time.</p> <p>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.</p>                                                      | 180 days |
| Device status is Critical                   | 4113 | KLSRV_HOST_STATUS_CRITICAL       | <p>Events of this type occur when a managed device is assigned the <i>Critical</i> status. You can <a href="#">configure the conditions</a> under which the device status is changed to <i>Critical</i>.</p>                                                                                                                                                                                | 180 days |
| The key file has been added to the denylist | 4124 | KLSRV_LICENSE_BLACKLISTED        | <p>Events of this type occur when Kaspersky has added the activation code or key file that you use to the denylist.</p> <p>Contact Technical Support for more details.</p>                                                                                                                                                                                                                  | 180 days |
| License expires soon                        | 4129 | KLSRV_EV_LICENSE_SRV_EXPIRE_SOON | <p>Events of this type occur when the <a href="#">commercial license</a> expiration date is approaching.</p>                                                                                                                                                                                                                                                                                | 180 days |

|                                |      |                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |
|--------------------------------|------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                |      |                           | <p>Once a day Kaspersky Security Center Linux checks whether a license expiration date is approaching. Events of this type are published 30 days, 15 days, 5 days, and 1 day before the license expiration date. This number of days cannot be changed. If the Administration Server is turned off on the specified day before the license expiration date, the event will not be published until the next day.</p> <p>When the commercial license expires, Kaspersky Security Center Linux provides only <a href="#">basic functionality</a>.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> <li>• Make sure that a <a href="#">reserve license key</a> is added to Administration Server.</li> <li>• If you use a <a href="#">subscription</a>, make sure to renew it. An unlimited subscription is renewed automatically if it has been prepaid to the service provider by the due date.</li> </ul> |          |
| <b>Certificate has expired</b> | 4132 | KLSRV_CERTIFICATE_EXPIRED | <p>Events of this type occur when the Administration Server certificate for Mobile Device Management expires.</p> <p>You need to update the expired certificate.</p> <p>You can configure automatic updates of certificates by selecting the <b>Reissue certificate automatically if possible</b> check box in the certificate issuance settings.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 180 days |

## Administration Server functional failure events

The table below shows the events of Kaspersky Security Center 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 |
|--------------------------------------------------------------------------------------|---------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Runtime error                                                                        | 4125          | KLSRV_RUNTIME_ERROR       | <p>Events of this type occur because of unknown issues.</p> <p>Most often these are DBMS issues, network issues, and other software and hardware issues.</p> <p>Details of the event can be found in the event description.</p>                                                                                                                                                                                                                                                                                                                                                                                                 | 180 days             |
| Limit of installations has been exceeded for one of the licensed applications groups | 4126          | KLSRV_INVLICPROD_EXCEEDED | <p>Administration Server generates events of this type periodically (every hour). Events of this type occur if in Kaspersky Security Center Linux you manage license keys of third-party applications and if the number of installations has exceeded the limit set by the license key of the third-party application.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> <li>• Look through the managed devices list. Delete the third-party application from devices on which the application is not in use.</li> <li>• Use a third-party license for more devices.</li> </ul> | 180 days             |

|                                                           |      |                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |          |
|-----------------------------------------------------------|------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                                           |      |                                 | 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.                                                                                                                                                                                                                                                                                                                                               |          |
| <b>Failed to copy the updates to the specified folder</b> | 4123 | KLSRV_UPD_REPL_FAIL             | <p>Events of this type occur when software updates are copied to an additional shared folder(s).</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> <li>• Check whether the user account that is employed to gain access to the folder(s) has write permission.</li> <li>• Check whether a user name and/or a password to the folder(s) changed.</li> <li>• Check the internet connection, as it might be the cause of the event. Follow the instructions to update databases and software modules.</li> </ul> | 180 days |
| <b>No free disk space</b>                                 | 4107 | KLSRV_DISK_FULL                 | <p>Events of this type occur when the hard drive of the device on which Administration Server is installed runs out of free space.</p> <p>Free up disk space on the device.</p>                                                                                                                                                                                                                                                                                                                                                                               | 180 days |
| <b>Shared folder is not available</b>                     | 4108 | KLSRV_SHARED_FOLDER_UNAVAILABLE | <p>Events of this type occur if the <a href="#">shared folder of Administration Server</a> is not available.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> <li>• Check whether the Administration Server (where the shared folder is located) is</li> </ul>                                                                                                                                                                                                                                               | 180 days |

|                                                            |      |                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |          |
|------------------------------------------------------------|------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                                            |      |                            | <p>turned on and available.</p> <ul style="list-style-type: none"> <li>• Check whether a user name and/or a password to the folder is/are changed.</li> <li>• Check the network connection.</li> </ul>                                                                                                                                                                                                                                                                                                        |          |
| <b>The Administration Server database is unavailable</b>   | 4109 | KLSRV_DATABASE_UNAVAILABLE | <p>Events of this type occur if the Administration Server database becomes unavailable.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> <li>• Check whether the remote server that has SQL Server installed is available.</li> <li>• View the DBMS logs to discover the reason for Administration Server database unavailability. For example, because of preventive maintenance a remote server with SQL Server installed might be unavailable.</li> </ul> | 180 days |
| <b>No free space in the Administration Server database</b> | 4110 | KLSRV_DATABASE_FULL        | <p>Events of this type occur when there is no free space in the Administration Server database.</p> <p>Administration Server does not function when its database has reached its capacity and when further recording to the database is not possible.</p> <p>Following are the causes of this event, depending on the DBMS that you use, and appropriate responses to the event:</p> <ul style="list-style-type: none"> <li>• You use the SQL Server Express Edition DBMS:</li> </ul>                         | 180 days |



- In the SQL Server Express documentation, review the database size limit for the version you use. Probably your Administration Server database has exceeded the database size limit.

- [Limit the number of events to store in the Administration Server database.](#)

- In the Administration Server database, there are too many events sent by the Application Control component. You can change the settings of the Kaspersky Endpoint Security policy relating to Application Control event storage in the Administration Server database.

- You use a DBMS other than SQL Server Express Edition:

- [Do not limit the number of events to store in the Administration Server database.](#)

- [Reduce the list of events to store in the Administration Server database.](#)

Review the information on [DBMS selection.](#)

The table below shows the events of Kaspersky Security Center 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.

Administration Server warning events

| Event type display name                   | Event type ID | Event type                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Default storage term |
|-------------------------------------------|---------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>A frequent event has been detected</b> |               | 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: <a href="#">Blocking frequent events</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 90 days              |
| <b>License limit has been exceeded</b>    | 4098          | KLSRV_EV_LICENSE_CHECK_100_110   | <p>Once a day Kaspersky Security Center Linux checks whether a licensing restriction is exceeded.</p> <p>Events of this type occur when Administration Server detects that some licensing limits are exceeded by Kaspersky applications installed on client devices and if the number of currently used <a href="#">licensing units</a> covered by a single license constitute 100% to 110% of the total number of units covered by the license.</p> <p>Even when this event occurs, client devices are protected.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> <li>• Look through the managed devices list. Delete devices that are not in use.</li> <li>• Provide a license for more devices (add a valid activation</li> </ul> | 90 days              |

|                                                                           |      |                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |         |
|---------------------------------------------------------------------------|------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                           |      |                               | <p>code or a key file to Administration Server).</p> <p>Kaspersky Security Center Linux determines <a href="#">the rules to generate events</a> when a licensing restriction is exceeded.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |         |
| <p><b>Device has remained inactive on the network for a long time</b></p> | 4103 | KLSRV_EVENT_HOSTS_NOT_VISIBLE | <p>Events of this type occur when a managed device shows inactivity for some time.</p> <p>Most often, this happens when a managed device is decommissioned.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> <li>• Manually remove the device from the list of managed devices. Specify the time interval after which the <b>Device has remained inactive on the network for a long time</b> event is created by <a href="#">using Kaspersky Security Center Web Console</a>.</li> <li>• Specify the time interval after which the device is automatically removed from the group by <a href="#">using Kaspersky Security Center Web Console</a>.</li> </ul> | 90 days |
| <p><b>Conflict of device names</b></p>                                    | 4102 | KLSRV_EVENT_HOSTS_CONFLICT    | <p>Events of this type occur when Administration Server considers two or more managed devices as a single device.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 90 days |

|                                                                                          |      |                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |         |
|------------------------------------------------------------------------------------------|------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                                          |      |                           | <p>Most often this happens when a cloned hard drive was used for software deployment on managed devices and without switching the Network Agent to the dedicated disk cloning mode on a reference device.</p> <p>To avoid this issue, switch Network Agent to the <a href="#">disk cloning mode</a> on a reference device before cloning the hard drive of this device.</p>                                                                                                                                                                                                                                                                                    |         |
| Device status is Warning                                                                 | 4114 | KLSRV_HOST_STATUS_WARNING | <p>Events of this type occur when a managed device is assigned the <i>Warning</i> status. You can <a href="#">configure the conditions</a> under which the device status is changed to <i>Warning</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 90 days |
| Limit of installations will soon be exceeded for one of the licensed applications groups | 4127 | KLSRV_INVLICPROD_FILLED   | <p>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.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> <li>• If the third-party application is not in use on some of the managed devices, delete the application from these devices.</li> <li>• 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</li> </ul> | 90 days |

|                                       |      |                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |         |
|---------------------------------------|------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                       |      |                             | <p>greater number of devices in advance.</p> <p>You can manage license keys of third-party applications using the functionality of licensed applications groups.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |         |
| <b>Certificate has been requested</b> | 4133 | KLSRV_CERTIFICATE_REQUESTED | <p>Events of this type occur when a certificate for Mobile Device Management fails to be automatically reissued.</p> <p>Following might be the causes and appropriate responses to the event:</p> <ul style="list-style-type: none"> <li>• Automatic reissue was initiated for a certificate for which the <b>Reissue certificate automatically if possible</b> 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.</li> <li>• 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.</li> </ul> | 90 days |
| <b>Certificate has been removed</b>   | 4134 | KLSRV_CERTIFICATE_REMOVED   | <p>Events of this type occur when an administrator removes any type of certificate (General, Mail, VPN) for Mobile Device Management.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 90 days |

|                                                            |      |                                    |                                                                                                                                                                                                                                                                                                                                                                                     |            |
|------------------------------------------------------------|------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|                                                            |      |                                    | <p>After removing a certificate, mobile devices connected via this certificate will fail to connect to Administration Server.</p> <p>This event might be helpful when investigating malfunctions associated with the management of mobile devices.</p>                                                                                                                              |            |
| <b>APNs certificate has expired</b>                        | 4135 | KLSRV_APN_CERTIFICATE_EXPIRED      | <p>Events of this type occur when an APNs certificate expires.</p> <p>You need to manually renew the APNs certificate and install it on an iOS MDM Server.</p>                                                                                                                                                                                                                      | Not stored |
| <b>APNs certificate expires soon</b>                       | 4136 | KLSRV_APN_CERTIFICATE_EXPIRES_SOON | <p>Events of this type occur when there are fewer than 14 days left before the APNs certificate expires.</p> <p>When the APNs certificate expires, you need to manually renew the APNs certificate and install it on an iOS MDM Server.</p> <p>We recommend that you schedule the APNs certificate renewal in advance of the expiration date.</p>                                   | Not stored |
| <b>Failed to send the FCM message to the mobile device</b> | 4138 | KLSRV_GCM_DEVICE_ERROR             | <p>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.</p> | 90 days    |

|                                                                    |      |                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |         |
|--------------------------------------------------------------------|------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                    |      |                      | <p>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 <a href="#">Google Firebase service documentation</a> (see chapter "Downstream message error response codes").</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |         |
| <p><b>HTTP error sending the FCM message to the FCM server</b></p> | 4139 | KLSRV_GCM_HTTP_ERROR | <p>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).</p> <p>Following might be the causes and appropriate responses to the event:</p> <ul style="list-style-type: none"> <li>• Problems on the FCM server side. 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 <a href="#">Google Firebase service documentation</a> (see chapter "Downstream message error response codes").</li> <li>• Problems on the proxy server side (if you use proxy server). Read the HTTP code in the</li> </ul> | 90 days |

|                                                                |      |                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |
|----------------------------------------------------------------|------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                |      |                            | details of the event and respond accordingly.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |         |
| <b>Failed to send the FCM message to the FCM server</b>        | 4140 | KLSRV_GCM_GENERAL_ERROR    | <p>Events of this type occur due to unexpected errors on the Administration Server side when working with the Google Firebase Cloud Messaging HTTP protocol.</p> <p>Read the details in the event description and respond accordingly.</p> <p>If you cannot find the solution to an issue on your own, we recommend that you contact Kaspersky Technical Support.</p>                                                                                                                                                                            | 90 days |
| <b>Little free space on the hard drive</b>                     | 4105 | KLSRV_NO_SPACE_ON_VOLUMES  | <p>Events of this type occur when the hard drive of the device on which Administration Server is installed almost runs out of free space.</p> <p>Free up disk space on the device.</p>                                                                                                                                                                                                                                                                                                                                                           | 90 days |
| <b>Little free space in the Administration Server database</b> | 4106 | KLSRV_NO_SPACE_IN_DATABASE | <p>Events of this type occur if space in the Administration Server database is too limited. If you do not remedy the situation, soon the Administration Server database will reach its capacity and Administration Server will not function.</p> <p>Following are the causes of this event, depending on the DBMS that you use, and the appropriate responses to the event.</p> <p>You use the SQL Server Express Edition DBMS:</p> <ul style="list-style-type: none"> <li>• In SQL Server Express documentation, review the database</li> </ul> | 90 days |



|                                                                                      |             |                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                |
|--------------------------------------------------------------------------------------|-------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|                                                                                      |             |                                        | <p>size limit for the version you use. Probably your Administration Server database is about to reach the database size limit.</p> <ul style="list-style-type: none"> <li>• <a href="#">Limit the number of events to store in the Administration Server database.</a></li> <li>• In the Administration Server database there are too many events sent by the Application Control component. You can change the settings of the Kaspersky Endpoint Security policy relating to Application Control event storage in the Administration Server database. You use a DBMS other than SQL Server Express Edition:</li> <li>• <a href="#">Do not limit the number of events to store in the Administration Server database</a></li> <li>• <a href="#">Reduce the list of events to store in the Administration Server database</a></li> </ul> <p>Review the information on <a href="#">DBMS selection</a>.</p> |                |
| <p><b>Connection to the secondary Administration Server has been interrupted</b></p> | <p>4116</p> | <p>KLSRV_EV_SLAVE_SRV_DISCONNECTED</p> | <p>Events of this type occur when a connection to the secondary Administration Server is interrupted.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <p>90 days</p> |

|                                                                                               |      |                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |            |
|-----------------------------------------------------------------------------------------------|------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|                                                                                               |      |                                  | Read the operating system log on the device where the secondary Administration Server is installed and respond accordingly.                                                                                                                                                                                                                                                                                                                                                                                        |            |
| Connection to the primary Administration Server has been interrupted                          | 4118 | KLSRV_EV_MASTER_SRV_DISCONNECTED | <p>Events of this type occur when a connection to the primary Administration Server is interrupted.</p> <p>Read the operating system log on the device where the primary Administration Server is installed and respond accordingly.</p>                                                                                                                                                                                                                                                                           | 90 days    |
| New updates for Kaspersky software modules have been registered                               | 4141 | KLSRV_SEAMLESS_UPDATE_REGISTERED | <p>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.</p> <p>Approve or decline the updates by using Kaspersky Security Center Web Console.</p>                                                                                                                                                                                                                                             | 90 days    |
| The limit on the number of events in the database is exceeded, deletion of events has started | 4145 | KLSRV_EVP_DB_TRUNCATING          | <p>Events of this type occur when deletion of old events from the Administration Server database has started after the <a href="#">Administration Server database capacity is reached</a>.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> <li>• <a href="#">Change the maximum number of events stored in the Administration Server database</a></li> <li>• <a href="#">Reduce the list of events to store in the Administration Server database</a></li> </ul> | Not stored |
| The limit on                                                                                  | 4146 | KLSRV_EVP_DB_TRUNCATED           | Events of this type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Not        |

|                                                                                       |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |               |
|---------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <p>the number of events in the database is exceeded, the events have been deleted</p> |  | <p>occur when old events have been deleted from the Administration Server database after the <a href="#">Administration Server database capacity is reached</a>.</p> <p>You can respond to the event in the following ways:</p> <ul style="list-style-type: none"> <li>• <a href="#">Change the allowed maximum number of events to be stored in the Administration Server database</a></li> <li>• <a href="#">Reduce the list of events to store in the Administration Server database</a></li> </ul> | <p>stored</p> |
|---------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|

## Administration Server informational events

The table below shows the events of Kaspersky Security Center 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                       | Default storage term | Remarks |
|---------------------------------------------------------------------------------|---------------|----------------------------------|----------------------|---------|
| Over 90% of the license key is used up                                          | 4097          | KLSRV_EV_LICENSE_CHECK_90        | 30 days              |         |
| New device has been detected                                                    | 4100          | KLSRV_EVENT_HOSTS_NEW_DETECTED   | 30 days              |         |
| Device has been automatically added to the group                                | 4101          | KLSRV_EVENT_HOSTS_NEW_REDIRECTED | 30 days              |         |
| Device has been removed from the group: inactive on the network for a long time | 4104          | KLSRV_INVISIBLE_HOSTS_REMOVED    | 30 days              |         |
| Limit of installations will soon be                                             | 4128          | KLSRV_INVLICPROD_EXPIRED_SOON    | 30 days              |         |

|                                                                                 |      |                                |         |                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------|------|--------------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| exceeded (more than 95% is used up) for one of the licensed applications groups |      |                                |         |                                                                                                                                                                                                                                                                                |
| 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 | 30 days |                                                                                                                                                                                                                                                                                |
| Updates have been successfully copied to the specified folder                   | 4122 | KLSRV_UPD_REPL_OK              | 30 days |                                                                                                                                                                                                                                                                                |
| Connection to the secondary Administration Server has been established          | 4115 | KLSRV_EV_SLAVE_SRV_CONNECTED   | 30 days |                                                                                                                                                                                                                                                                                |
| Connection to the primary Administration Server has been established            | 4117 | KLSRV_EV_MASTER_SRV_CONNECTED  | 30 days |                                                                                                                                                                                                                                                                                |
| Databases have been updated                                                     | 4144 | KLSRV_UPD_BASES_UPDATED        | 30 days |                                                                                                                                                                                                                                                                                |
| Audit: Connection to the Administration Server has been established             | 4147 | KLAUD_EV_SERVERCONNECT         | 30 days |                                                                                                                                                                                                                                                                                |
| Audit: Object has been modified                                                 | 4148 | KLAUD_EV_OBJECTMODIFY          | 30 days | <p>This event tracks changes in the following objects:</p> <ul style="list-style-type: none"> <li>• Administration group</li> <li>• Security group</li> <li>• User</li> <li>• Package</li> <li>• Task</li> <li>• Policy</li> <li>• Server</li> <li>• Virtual Server</li> </ul> |

|                                                                                         |      |                             |         |                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------|------|-----------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Audit: Object status has changed</b>                                                 | 4150 | KLAUD_EV_TASK_STATE_CHANGED | 30 days | For example, this event occurs when a task has failed with an error.                                                                                                           |
| <b>Audit: Group settings have been modified</b>                                         | 4149 | KLAUD_EV_ADMGROUP_CHANGED   | 30 days |                                                                                                                                                                                |
| <b>Audit: Connection to Administration Server has been terminated</b>                   | 4151 | KLAUD_EV_SERVERDISCONNECT   | 30 days |                                                                                                                                                                                |
| <b>Audit: Object properties have been modified</b>                                      | 4152 | KLAUD_EV_OBJECTPROPMODIFIED | 30 days | This event tracks changes in the following properties: <ul style="list-style-type: none"> <li>• User</li> <li>• License</li> <li>• Server</li> <li>• Virtual server</li> </ul> |
| <b>Audit: User permissions have been modified</b>                                       | 4153 | KLAUD_EV_OBJECTACLMODIFIED  | 30 days |                                                                                                                                                                                |
| <b>Audit: Encryption keys have been imported or exported from Administration Server</b> | 5100 | KLAUD_EV_DPEKEYSEXPORT      | 30 days |                                                                                                                                                                                |

## Network Agent events

This section contains information about the events related to Network Agent.

### Network Agent warning events

The table below shows the events of Network Agent that have the **Warning** severity level.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. If you want to configure notification settings for all the events at once, [configure general notification settings](#) in the Administration Server properties.

Network Agent warning events

| Event type display name | Event type ID | Event type | Default storage |
|-------------------------|---------------|------------|-----------------|
|-------------------------|---------------|------------|-----------------|

|                                                             |      |                                 | term    |
|-------------------------------------------------------------|------|---------------------------------|---------|
| Security issue has occurred                                 | 549  | GNRL_EV_APP_INCIDENT_OCCURED    | 30 days |
| KSN Proxy has started. Failed to check KSN for availability | 7718 | KSNPROXY_STARTED_CON_CHK_FAILED | 30 days |

## Network Agent informational events

The table below shows the events of Network Agent that have the **Info** severity level.

For each event that can be generated by an application, you can specify notification settings and storage settings on the **Event configuration** tab in the application policy. If you want to configure notification settings for all the events at once, [configure general notification settings](#) in the Administration Server properties.

Network Agent informational events

| Event type display name                                                  | Event type ID | Event type                       | Default storage term |
|--------------------------------------------------------------------------|---------------|----------------------------------|----------------------|
| Application has been installed                                           | 7703          | KLNAG_EV_INV_APP_INSTALLED       | 30 days              |
| Application has been uninstalled                                         | 7704          | KLNAG_EV_INV_APP_UNINSTALLED     | 30 days              |
| Monitored application has been installed                                 | 7705          | KLNAG_EV_INV_OBS_APP_INSTALLED   | 30 days              |
| Monitored application has been uninstalled                               | 7706          | KLNAG_EV_INV_OBS_APP_UNINSTALLED | 30 days              |
| New device has been added                                                | 7708          | KLNAG_EV_DEVICE_ARRIVAL          | 30 days              |
| Device has been removed                                                  | 7709          | KLNAG_EV_DEVICE_REMOVE           | 30 days              |
| New device has been detected                                             | 7710          | KLNAG_EV_NAC_DEVICE_DISCOVERED   | 30 days              |
| Device has been authorized                                               | 7711          | KLNAG_EV_NAC_HOST_AUTHORIZED     | 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 Security Center Web Console interface, for configuration.

Event selections are available in the Kaspersky Security Center Web Console, in the **Monitoring & reporting** section, by clicking **Event selections**.

By default, event selections include information for the last seven days.

Kaspersky Security Center Linux has a default set of event (predefined) selections:

- Events with different importance levels:
  - **Critical events**
  - **Functional failures**
  - **Warnings**
  - **Informational messages**
- **User requests** (events of managed applications)
- **Recent events** (over the last week)
- [Audit events](#).

You can also [create and configure additional user-defined selections](#). In user-defined selections, you can filter events by the properties of the devices they originated from (device names, IP ranges, and administration groups), by event types and severity levels, by application and component name, and by time interval. It is also possible to include task results in the search scope. You can also use a simple search field where a word or several words can be typed. All events that contain any of the typed words anywhere in their attributes (such as event name, description, component name) are displayed.

Both for predefined and user-defined selections, you can limit the number of displayed events or the number of records to search. Both options affect the time it takes Kaspersky Security Center Linux to display the events. The larger the database is, the more time-consuming the process can be.

You can do the following:

- [Edit properties of event selections](#)
- [Generate event selections](#)
- [View details of event selections](#)
- [Delete event selections](#)
- [Delete events from the Administration Server database](#)

## Creating an event selection

*To create an event selection:*

1. In the main menu, go to **Monitoring & reporting** → **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 the changes.  
The confirmation window opens.
5. To view the event selection result, keep the **Go to selection result** check box selected.
6. Click **Save** to confirm the event selection creation.

If you kept the **Go to selection result** check box selected, the event selection result is displayed. Otherwise, the new event selection appears in the list of event selections.

## Editing an event selection

*To edit an event selection:*

1. In the main menu, go to **Monitoring & reporting** → **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 the 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 **Monitoring & reporting** → **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 Security Center Linux allows you to save an event selection and its settings to a KLO file. You can use this KLO file to [import the saved event selection](#) both to Kaspersky Security Center Windows and Kaspersky Security Center Linux.

Note that you can export only user-defined event selections. Event selections from the default set of Kaspersky Security Center Linux (predefined selections) cannot be saved to a file.

*To export an event selection:*

1. In the main menu, go to **Monitoring & reporting** → **Event selections**.
2. Select the check box next to the event selection that you want to export.

You cannot export multiple event selections at the same time. If you select more than one selection, the **Export** button will be disabled.
3. Click the **Export** button.
4. In the opened **Save as** window, specify the event selection file name and path, and then click the **Save** button.

The **Save as** window is displayed only if you use Google Chrome, Microsoft Edge, or Opera. If you use another browser, the event selection file is automatically saved in the **Downloads** folder.

## Importing an event selection

Kaspersky Security Center Linux allows you to import an event selection from a KLO file. The KLO file contains the [exported event selection](#) and its settings.

*To import an event selection:*

1. In the main menu, go to **Monitoring & reporting** → **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

*To export events to a file:*

1. [Start an event selection.](#)

2. Select the check box next to the required event.

3. Click the **Export to file** button.

The selected event is exported to a 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.

## Deleting events

*To delete one or several events:*

1. [Start an event selection](#).
2. Select the check boxes next to the required events.
3. 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 & reporting** → **Event selections**.
2. Select the check boxes next to the event selections that you want to delete.
3. Click **Delete**.
4. In the window that opens, click **OK**.

The event selection is deleted.

## Setting the storage term for an event

Kaspersky Security Center Linux allows you to receive information about events that occur during the operation of Administration Server and Kaspersky applications installed on managed devices. Information about events is saved in the Administration Server database. You might need to store some events for a longer or shorter period of time than specified by default values. You can change the default settings of the storage term for an event.

If you are not interested in storing some events in the database of Administration Server, you can disable the appropriate setting in the Administration Server policy and Kaspersky application policy, or in the Administration Server properties (only for Administration Server events). This will reduce the number of event types in the database.

The longer the storage term for an event, the faster the database reaches its maximum capacity. However, a longer storage term for an event lets you perform monitoring and reporting tasks for a longer period of time.

*To set the storage term for an event in the database of Administration Server:*

1. In the main menu, go to **Assets (Devices) → Policies & profiles**.
2. Do one of the following:
  - To configure the storage term of the events of Network Agent or of a managed Kaspersky application, click the name of the corresponding policy.  
The policy properties page opens.
  - To configure Administration Server events, in the main menu, click the settings icon (⚙) next to the name of the required Administration Server.  
If you have a policy for the Administration Server, you can click the name of this policy instead.  
The Administration Server properties page (or the Administration Server policy properties page) opens.
3. Select the **Event configuration** tab.  
A list of event types related to the **Critical** section is displayed.
4. Select the **Functional failure**, **Warning**, or **Info** section.
5. In the list of event types in the right pane, click the link for the event whose storage term you want to change.  
In the **Event registration** section of the window that opens, the **Store in the Administration Server database for (days)** option is enabled.
6. In the edit box below this toggle button, enter the number of days to store the event.
7. If you do not want to store an event in the Administration Server database, disable the **Store in the Administration Server database for (days)** option.

If you configure Administration Server events in Administration Server properties window and if event settings are locked in the Kaspersky Security Center Administration Server policy, you cannot redefine the storage term value for an event.

8. Click **OK**.

The properties window of the policy is closed.

From now on, when Administration Server receives and stores the events of the selected type, they will have the changed storage term. Administration Server does not change the storage term of previously received events.

## Blocking frequent events

This section provides information about managing frequent events blocking and about removing blocking of frequent events.

### About blocking frequent events

A managed application, for example, Kaspersky Endpoint Security for Linux, installed on a single or several managed devices can send a lot of events of the same type to the Administration Server. Receiving frequent events may overload the Administration Server database and overwrite other events. Administration Server starts blocking the most frequent events when the number of all the received events exceeds the [specified limit for the database](#).

Administration Server blocks the frequent events from receiving automatically. You cannot block the frequent events yourself, or choose which events to block.

If you want to find out if an event is blocked, you can view the notification list or you can check if this event is present in the **Blocking frequent events** section of the Administration Server properties. If the event is blocked, you can do the following:

- If you want to prevent overwriting the database, you can [continue blocking](#) such type of events from receiving.
- If you want, for example, to find the reason of sending the frequent events to the Administration Server, you can [unblock](#) frequent events and continue receiving the events of this type anyway.
- If you want to continue receiving the frequent events until they become blocked again, you can [remove from blocking](#) the frequent events.

### Managing frequent events blocking

Administration Server blocks the automatic receiving of frequent events, but you can unblock and continue to receive frequent events. You can also block receiving frequent events that you unblocked before.

*To manage frequent events blocking:*

1. In the main menu, click the 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.

## Event processing and storage on the Administration Server

Information about events during the operation of the application and managed devices is saved in the Administration Server database. Each event is attributed to a certain type and level of severity (*Critical event*, *Functional failure*, *Warning*, or *Info*). Depending on the conditions under which an event occurred, the application can assign different levels of severity to events of the same type.

You can view types and levels of severity assigned to events in the **Event configuration** section of the Administration Server properties window. In the **Event configuration** section, you can also configure processing of every event by the Administration Server:

- Registration of events on the Administration Server and in event logs of the operating system on a device and on the Administration Server.
- Method used for notifying the administrator of an event (for example, an SMS or email message).

In the **Events repository** section of the Administration Server properties window, you can edit the settings of events storage in the Administration Server database by limiting the number of event records and record storage term. When you specify the maximum number of events, the application calculates an approximate amount of storage space required for the specified number. You can use this approximate calculation to evaluate whether you have enough free space on the disk to avoid database overflow. The default capacity of the Administration Server database is 400,000 events. The maximum recommended capacity of the database is 45 million events.

The application checks the database every 10 minutes. If the number of events reaches the specified maximum value plus 10,000, the application deletes the oldest events so that only the specified maximum number of events remains.

When the Administration Server deletes old events, it cannot save new events to the database. During this period of time, information about events that were rejected is written to the operating system log. The new events are queued and then saved to the database after the deletion operation is complete.

## Notifications and device statuses

This section contains information on how to view notifications, configure notification delivery, use device statuses, and enable changing device statuses.

### Using notifications

Notifications alert you about events and help you to speed up your responses to these events by performing recommended actions or actions you consider as appropriate.

Depending on the notification method chosen, the following types of notifications are available:

- Onscreen notifications
- Notifications by SMS
- Notifications by email
- Notifications by executable file or script

#### Onscreen notifications

Onscreen notifications alert you to events grouped by importance levels (*Critical*, *Warning*, and *Informational*).

Onscreen notification can have one of two statuses:

- *Reviewed*. It means you have performed recommended action for the notification or you have assigned this status for the notification manually.
- *Not Reviewed*. It means you have not performed recommended action for the notification or you have not assigned this status for the notification manually.

By default, the list of notifications include notifications in the *Not Reviewed* status.

You can monitor your organization's network [viewing onscreen notifications](#) and responding to them in a real time.

#### Notifications by email, by SMS, and by executable file or a script

Kaspersky Security Center Linux provides the capability to monitor your organization's network by sending notifications about any event that you consider important. For any event you can [configure notifications by email, by SMS, or by running an executable file or a script](#).

Upon receiving notifications by email or by SMS, you can decide on your response to an event. This response should be the most appropriate for your organization's network. By running an executable file or a script, you predefine a response to an event. You can also consider running an executable file or a script as a primary response to an event. After the executable file runs, you can take other steps to respond to the event.

## Viewing onscreen notifications

You can view notifications onscreen in three ways:

- In the **Monitoring & reporting** → **Notifications** section. Here you can view notifications relating to predefined categories.
- In a separate window that can be opened no matter which section you are using at the moment. In this case you can mark notifications as reviewed.
- In the **Notifications by selected severity level** widget on the **Monitoring & reporting** → **Dashboard** section. In the widget, you can view only notifications of events that are at the *Critical* and *Warning* importance levels.

You can perform actions, for example, you can respond to an event.

*To view notifications from predefined categories:*

1. In the main menu, go to **Monitoring & reporting** → **Notifications**.

The **All notifications** category is selected in the left pane, and in the right pane all the notifications are displayed.

2. In the left pane, select one of the categories:

- **Deployment**
- **Devices**
- **Protection**
- **Updates** (this includes notifications about Kaspersky applications available for download and notifications about anti-virus database updates that have been downloaded)
- **Exploit Prevention**
- **Administration Server** (this includes events concerning only Administration Server)
- **Useful links** (this includes links to Kaspersky resources, for example, Kaspersky Technical Support, Kaspersky forum, license renewal page, or the Kaspersky IT Encyclopedia)
- **Kaspersky news** (this includes information about releases of Kaspersky applications)

A list of notifications of the selected category is displayed. The list contains the following:

- Icon related to the topic of the notification: deployment (📦), protection (🛡️), updates (🔄), device management (📱), Exploit Prevention (🔍), Administration Server (🏢).
- Notification importance level. Notifications of the following importance levels are displayed: **Critical notifications** (🔴), **Warning notifications** (🟡), **Info notifications**. Notifications in the list are grouped by importance levels.



- **Notification.** This contains a description of the notification.
- **Action.** This contains a link to a quick action that we recommend you perform. For example, by clicking this link, you can [proceed to the repository](#) and install security applications on devices, or view a list of devices or a list of events. After you perform the recommended action for the notification, this notification is assigned the *Reviewed* status.
- **Status registered.** This contains the number of days or hours that have passed from the moment when the notification was registered on the Administration Server.

To view onscreen notifications in a separate window by importance level:

1. In the upper-right corner of Kaspersky Security Center Web Console, click the flag icon (🚩).

If the flag icon has a red dot, there are notifications that have not been reviewed.

A window opens listing the notifications. By default, the **All notifications** tab is selected and the notifications are grouped by importance level: *Critical*, *Warning*, and *Info*.

2. Select the **System** tab.

The list of *Critical* (🔴) and *Warning* (⚠️) importance levels notifications is displayed. The notification list includes the following:

- Color marker. Critical notifications are marked in red. Warning notifications are marked in yellow.
- Icon indicating the topic of the notification: deployment (📦), protection (🛡️), updates (🔄), device management (🖨️), Exploit Prevention (🛑), Administration Server (🏢).
- Description of the notification.
- Flag icon. The flag icon is gray if notifications have been assigned the *Not Reviewed* status. When you select the gray flag icon and assign the *Reviewed* status to a notification, the icon changes color to white.
- Link to the recommended action. When you perform the recommended action after clicking the link, the notification gets the *Reviewed* status.
- Number of days that have passed since the date when the notification was registered on the Administration Server.

3. Select the **More** tab.

The list of *Info* importance level notifications is displayed.

The organization of the list is the same as for the list on the **System** tab (see the description above). The only difference is the absence of a color marker.

You can filter notifications by the date interval when they were registered on Administration Server. Use the **Show filter** check box to manage the filter.

To view onscreen notifications in the widget:

1. In the **Dashboard** section, select **Add or restore web widget**.
2. In the window that opens, click the **Other** category, select the **Notifications by selected severity level** widget, and click [Add](#).

The widget now appears on the **Dashboard** tab. By default, the notifications of *Critical* importance level are displayed on the widget.

You can click the **Settings** button on the widget and [change the widget settings](#) to view notifications of the *Warning* importance level. Or, you can add another widget: **Notifications by selected severity level**, with a *Warning* importance level.

The list of notifications on the widget is limited by its size and includes two notifications. These two notifications relate to the latest events.

The notification list in the widget includes the following:

- Icon related to the topic of the notification: deployment (📦), protection (🛡️), updates (🔄), device management (📱), Exploit Prevention (🛡️), Administration Server (🖨️).
- Description of the notification with a link to the recommended action. When you perform a recommended action after clicking the link, the notification gets the *Reviewed* status.
- Number of days or number of hours that have passed since the date when the notification was registered on the Administration Server.
- Link to other notifications. Upon clicking this link, you are transferred to the view of notifications in the **Notifications** section of the **Monitoring & reporting** section.

## About device statuses

Kaspersky Security Center Linux assigns a status to each managed device. The particular status depends on whether the conditions defined by the user are met. In some cases, when assigning a status to a device, Kaspersky Security Center Linux takes into consideration the device's visibility flag on the network (see the table below). If Kaspersky Security Center Linux does not find a device on the network within two hours, the visibility flag of the device is set to *Not Visible*.

The statuses are the following:

- *Critical* or *Critical/Visible*
- *Warning* or *Warning/Visible*
- *OK* or *OK/Visible*

The table below lists the default conditions that must be met to assign the *Critical* or *Warning* status to a device, with all possible values.

Conditions for assigning a status to a device

| Condition                             | Condition description                                                                  | Available values                                                                                          |
|---------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Security application is not installed | Network Agent is installed on the device, but a security application is not installed. | <ul style="list-style-type: none"> <li>• Toggle button is on.</li> <li>• Toggle button is off.</li> </ul> |
| Too many                              | Some viruses have been found on the device by a task for virus                         | More than 0.                                                                                              |

|                                                                            |                                                                                                                                                                                                                                                                                                                                      |                                                                                                                             |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| viruses detected                                                           | detection, for example, the Malware scan task, and the number of viruses found exceeds the specified value.                                                                                                                                                                                                                          |                                                                                                                             |
| 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.                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• Stopped.</li> <li>• Paused.</li> <li>• Running.</li> </ul>                         |
| 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 <i>Malware scan</i> 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 <b>Active threats</b> 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.                                                                                                                                                                         | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                   |
| License expired                                                            | The device is visible on the network, but the license has expired.                                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                   |
| License expires soon                                                       | The device is visible on the network, but the license will expire on the device in less than the specified number of days.                                                                                                                                                                                                           | More than 0 days.                                                                                                           |
| Invalid encryption status                                                  | Network Agent is installed on the device, but the device encryption result is equal to the specified value.                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• Does not comply with the policy due to the user's refusal (for external</li> </ul> |

|                                      |                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                  |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                      |                                                                                                                                                                                                                                                                                                                                                                                  | <p>devices only).</p> <ul style="list-style-type: none"> <li>• Does not comply with the policy due to an error.</li> <li>• Restart is required when applying the policy.</li> <li>• No encryption policy is specified.</li> <li>• Not supported.</li> <li>• When applying the policy.</li> </ul> |
| 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.                                                                                                                                                    | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                                                                                                                                                                                        |
| Device status defined by application | The status of the device is defined by the managed application.                                                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                                                                                                                                                                                        |
| 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 <i>Critical</i> or <i>Warning</i> status is changed to the <i>OK</i> 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.                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul>                                                                                                                                                                                        |
| Protection is                        | The device is visible on the network, but the security application on the                                                                                                                                                                                                                                                                                                        | More than 0                                                                                                                                                                                                                                                                                      |

|                                     |                                                                                                                                                                                                                                                             |                                                                                                           |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| disabled                            | device has been disabled for longer than the specified time interval.<br>In this case, the state of the security application is <i>stopped</i> or <i>failure</i> , and differs from the following: <i>starting</i> , <i>running</i> , or <i>suspended</i> . | 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.                                                                                                                                              | <ul style="list-style-type: none"> <li>• Toggle button is off.</li> <li>• Toggle button is on.</li> </ul> |

Kaspersky Security Center Linux allows you to set up automatic switching of the status of a device in an administration group when specified conditions are met. When the specified conditions are met, the client device is assigned one of the following statuses: *Critical* or *Warning*. When the specified conditions are not met, the client device is assigned the *OK* status.

Different statuses may correspond to different values of one condition. For example, by default, if the **Databases are outdated** condition has the **More than 3 days** value, the client device is assigned the *Warning* status; if the value is **More than 7 days**, the *Critical* status is assigned.

If you upgrade Kaspersky Security Center Linux from the previous version, the values of the **Databases are outdated** condition for assigning the status to *Critical* or *Warning* do not change.

When Kaspersky Security Center Linux 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 **Assets (Devices)** → **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 these 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 **Assets (Devices)** → **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 these 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 notification about events occurring in Kaspersky Security Center Linux. Depending on the notification method chosen, the following types of notifications are available:

- **Email**—When an event occurs, Kaspersky Security Center Linux sends a notification to the email addresses specified.
- **SMS**—When an event occurs, Kaspersky Security Center Linux sends a notification to the phone numbers specified.
- **Executable file**—When an event occurs, the executable file is run on the Administration Server.

*To configure notification delivery of events occurring in Kaspersky Security Center Linux:*

1. In the main menu, click the settings icon (⚙️) next to the name of the required Administration Server.  
The Administration Server properties window opens with the **General** tab selected.

2. Click the **Notification** section, and in the right pane select the tab for the notification method you want:

- [Email](#) 

The **Email** tab allows you to configure event notification by email.

In the **SMTP servers** field, specify mail server addresses, separating them with semicolons. You can use the following values:

- IPv4 or IPv6 address
- DNS name of the SMTP server

In the **SMTP server port** field, specify the number of an SMTP server communication port. The default port number is 25.

If you enable the **Use DNS MX lookup** option, you can use several MX records of the IP addresses for the same DNS name of the SMTP server. The same DNS name may have several MX records with different values of priority of receiving email messages. Administration Server attempts to send email notifications to the SMTP server in ascending order of MX records priority.

If you enable the **Use DNS MX lookup** option and do not enable usage of TLS settings, we recommend that you use the DNSSEC settings on your server device as an additional measure of protection for sending email notifications.

If you enable the **Use ESMTP authentication** option, you can specify the ESMTP authentication settings in the **User name** and **Password** fields. By default, the option is disabled, and the ESMTP authentication settings are not available.

You can specify TLS settings of connection with an SMTP server:

- **Do not use TLS**

You can select this option if you want to disable encryption of email messages.

- **Use TLS if supported by the SMTP server**

You can select this option if you want to use a TLS connection to an SMTP server. If the SMTP server does not support TLS, Administration Server connects the SMTP server without using TLS.

- **Always use TLS, check server certificate validity**

You can select this option if you want to use TLS authentication settings. If the SMTP server does not support TLS, Administration Server cannot connect the SMTP server.

We recommend that you use this option for better protection of the connection with an SMTP server. If you select this option, you can set authentication settings for a TLS connection.

If you select **Always use TLS, check server certificate validity** value, you can specify a certificate for authentication of the SMTP server and choose whether you want to enable communication through any version of TLS or only through TLS 1.2 or later versions. Also, you can specify a certificate for client authentication on the SMTP server.

You can specify certificates for a TLS connection by clicking the **Specify certificates** link:

- Browse for an SMTP server certificate file:

You can receive a file with the list of certificates from a trusted certification authority and upload the file to Administration Server. Kaspersky Security Center Linux checks whether the certificate of an SMTP server is also signed by a trusted certification authority. Kaspersky Security Center Linux cannot connect to an SMTP server if the certificate of the SMTP server is not received from a trusted certification authority.

- Browse for a client certificate file:

You can use a certificate that you received from any source, for example, from any trusted certification authority. You must specify the certificate and its private key by using one of the following certificate types:



- X-509 certificate:

You must specify a file with the certificate and a file with the private key. Both files do not depend on each other and the order of loading of the files is not significant. When both files are loaded, you must specify the password for decoding the private key. The password can have an empty value if the private key is not encoded.

- pkcs12 container:

You must upload a single file that contains the certificate and its private key. When the file is loaded, you must then specify the password for decoding the private key. The password can have an empty value if the private key is not encoded.

Clicking the **Send test message** button allows you to check whether you configured notifications properly: the application sends a test notification to the email addresses that you specified.

In the **Recipients (email addresses)** field, specify the email addresses to which the application will send notifications. You can specify multiple addresses in this field, by separating them with semicolons.

In the **Subject** field, specify the email subject. You can leave this field empty.

In the **Subject template** drop-down list, select the template for your subject. A variable determined by the selected template is placed automatically in the **Subject** field. You can construct an email subject selecting several subject templates.

In the **Sender email address: If this setting is not specified, the recipient address will be used instead. Warning: We do not recommend using a fictitious email address** field, specify the sender email address. If you leave this field empty, by default, the recipient address is used. It is not recommended to use fictitious email addresses.

The **Notification message** field contains standard text with information about the event that the application sends when an event occurs. This text includes substitute parameters, such as event name, device name, and domain name. You can edit the message text by adding other [substitute parameters](#) with more relevant details about the event.

If the notification text contains a percent sign (%), you have to type it twice in a row to allow message sending. For example, "CPU load is 100%%".

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send during the specified time interval.

- [SMS](#) 

The **SMS** tab allows you to configure the transmission of SMS notifications about various events to a cell phone. SMS messages are sent through a mail gateway.

In the **SMTP servers** field, specify mail server addresses, separating them with semicolons. You can use the following values:

- IPv4 or IPv6 address
- DNS name of the SMTP server

In the **SMTP server port** field, specify the number of an SMTP server communication port. The default port number is 25.

If the **Use ESMTP authentication** option is enabled, you can specify the ESMTP authentication settings in the **User name** and **Password** fields. By default, the option is disabled, and the ESMTP authentication settings are not available.

You can specify TLS settings of connection with an SMTP server:

- **Do not use TLS**

You can select this option if you want to disable encryption of email messages.

- **Use TLS if supported by the SMTP server**

You can select this option if you want to use a TLS connection to an SMTP server. If the SMTP server does not support TLS, Administration Server connects the SMTP server without using TLS.

- **Always use TLS, check server certificate validity**

You can select this option if you want to use TLS authentication settings. If the SMTP server does not support TLS, Administration Server cannot connect the SMTP server.

We recommend that you use this option for better protection of the connection with an SMTP server. If you select this option, you can set authentication settings for a TLS connection.

If you select **Always use TLS, check server certificate validity** value, you can specify a certificate for authentication of the SMTP server and choose whether you want to enable communication through any version of TLS or only through TLS 1.2 or later versions. Also, you can specify a certificate for client authentication on the SMTP server.

You can specify SMTP server certificate file by clicking the **Specify certificates** link. You can receive a file with the list of certificates from a trusted certification authority and upload the file to Administration Server. Kaspersky Security Center Linux checks whether the certificate of an SMTP server is also signed by a trusted certification authority. Kaspersky Security Center Linux cannot connect to an SMTP server if the certificate of the SMTP server is not received from a trusted certification authority.

In the **Recipients (email addresses)** field, specify the email addresses to which the application will send notifications. You can specify multiple addresses in this field, by separating them with semicolons. The notifications will be delivered to the phone numbers associated with the specified email addresses.

In the **Subject** field, specify the email subject.

In the **Subject template** drop-down list, select the template for your subject. A variable according to the selected template is put in the **Subject** field. You can construct an email subject selecting several subject templates.

In the **Sender email address: If this setting is not specified, the recipient address will be used instead.** **Warning: We do not recommend using a fictitious email address** field, specify the sender email address. If you leave this field empty, by default, the recipient address is used. It is not recommended to use fictitious email addresses.

In the **Phone numbers of SMS message recipients** field, specify the cell phone numbers of the SMS notification recipients.

In the **Notification message** field, specify a text with information about the event that the application sends when an event occurs. This text can include [substitute parameters](#), such as event name, device name, and domain name.

If the notification text contains a percent sign (%), you have to type it twice in a row to allow message sending. For example, "CPU load is 100%%".

Click the **Send test message** to check whether you configured notifications properly: the application sends a test notification to the recipient that you specified.

Click the **Configure numeric limit of notifications** link to specify the maximum number of notifications that the application can send during the specified time interval.

- [Executable file to be run](#) 

If this notification method is selected, in the entry field you can specify the application that will start when an event occurs.

In the **Executable file to be run on the Administration Server when an event occurs** field, specify the folder and the name of the file to be run. Before specifying the file, [prepare the file and specify the placeholders](#) that define the event details to be sent in the notification message. The folder and the file that you specify must be located on the Administration Server.

Clicking the **Configure numeric limit of notifications** link allows you to specify the maximum number of notifications that the application can send during the specified time interval.

3. On the tab, define the notification settings.

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 Security Center Linux.

You can [override notification delivery settings](#) for certain events in the **Event configuration** section of the Administration Server settings, of a policy's settings, or of an application's settings.

## Testing notifications

To check whether event notifications are sent, the application uses the notification of the EICAR test virus detection on client devices.

*To verify sending of event notifications:*

1. Stop the real-time file system protection task on a client device and copy the EICAR test virus to that client device. Then, re-enable real-time protection of the file system.
2. Run a scan task for client devices in an administration group or for specific devices, including one with the EICAR test virus.

If the scan task is configured correctly, the test virus will be detected. If notifications are configured correctly, you are notified that a virus has been detected.

*To open a record of the test virus detection:*

1. In the main menu, go to **Monitoring & reporting** → **Event selections**.

2. Click the **Recent events** selection name.

In the window that opens, the notification about the test virus is displayed.

The EICAR test virus contains no code that can do harm to your device. However, most manufacturers' security applications identify this file as a virus. You can download the test virus from the [official EICAR website](#).

## Event notifications displayed by running an executable file

Kaspersky Security Center Linux can notify the administrator about events on client devices by running an executable file. The executable file must contain another executable file with placeholders of the event to be relayed to the administrator.

Placeholders for describing an event

| Placeholder                      | Placeholder description                     |
|----------------------------------|---------------------------------------------|
| %SEVERITY%                       | Event importance level                      |
| %COMPUTER%                       | Name of the device where the event occurred |
| %DOMAIN%                         | Domain                                      |
| %EVENT%                          | Event                                       |
| %DESCR%                          | Event description                           |
| %RISE_TIME%                      | Time created                                |
| %KLCSAK_EVENT_TASK_DISPLAY_NAME% | Task name                                   |
| %KL_PRODUCT%                     | Network Agent                               |
| %KL_VERSION%                     | Network Agent version number                |
| %HOST_IP%                        | IP address                                  |
| %HOST_CONN_IP%                   | Connection IP address                       |

### Example:

Event notifications are sent by an executable file (such as script1.bat) inside which another executable file (such as script2.bat) with the %COMPUTER% placeholder is launched. When an event occurs, the script1.bat file is run on the administrator's device, which, in turn, runs the script2.bat file with the %COMPUTER% placeholder. The administrator then receives the name of the device where the event occurred.

## Kaspersky announcements

This section describes how to use, configure, and disable Kaspersky announcements.

## About Kaspersky announcements

The Kaspersky announcements section (**Monitoring & reporting** → **Kaspersky announcements**) keeps you informed by providing information related to your version of Kaspersky Security Center Linux and the managed applications installed on the managed devices. Kaspersky Security Center Linux periodically updates the information in the section by removing outdated announcements and adding new information.

Kaspersky Security Center Linux shows only those Kaspersky announcements that relate to the currently connected Administration Server and the Kaspersky applications installed on the managed devices of this Administration Server. The announcements are shown individually for any type of Administration Server—primary, secondary, or virtual.

Administration Server must have an internet connection to receive Kaspersky announcements.

The announcements include information of the following types:

- Security-related announcements

Security-related announcements are intended to keep the Kaspersky applications installed in your network up-to-date and fully functional. The announcements may include information about critical updates for Kaspersky applications, fixes for found vulnerabilities, and ways to fix other issues in Kaspersky applications. By default, security-related announcements are enabled. If you do not want to receive the announcements, you can [disable this feature](#).

To show you the information that corresponds to your network protection configuration, Kaspersky Security Center Linux sends data to Kaspersky cloud servers and receives only those announcements that relate to the Kaspersky applications installed in your network. The data set that can be sent to the servers is described in the [End User License Agreement](#) that you accept when you install Kaspersky Security Center Administration Server.

- Marketing announcements

Marketing announcements include information about special offers for your Kaspersky applications, advertisements, and news from Kaspersky. Marketing announcements are disabled by default. You receive this type of announcements only if you enabled Kaspersky Security Network (KSN). You can [disable marketing announcements](#) by disabling KSN.

To show you only relevant information that might be helpful in protecting your network devices and in your everyday tasks, Kaspersky Security Center Linux sends data to Kaspersky cloud servers and receives the appropriate announcements. The data set that can be sent to the servers is described in the Processed Data section of the [KSN Statement](#).

New information is divided into the following categories, according to importance:

1. Critical info
2. Important news
3. Warning
4. Info

When new information appears in the Kaspersky announcements section, Kaspersky Security Center Web Console displays a notification label that corresponds to the importance level of the announcements. You can click the label to view this announcement in the Kaspersky announcements section.

You can specify the [Kaspersky announcements settings](#), including the announcement categories that you want to view and where to display the notification label. If you do not want to receive announcements, you can [disable this feature](#).

## Specifying Kaspersky announcements settings

In the [Kaspersky announcements](#) section, you can specify the Kaspersky announcements settings, including the categories of the announcements that you want to view and where to display the notification label.

*To configure Kaspersky announcements:*

1. In the main menu, go to **Monitoring & reporting** → **Kaspersky announcements**.

2. Click the **Settings** link.

The Kaspersky announcement settings window opens.

3. Specify the following settings:

- Select the importance level of the announcements that you want to view. The announcements of other categories will not be displayed.
- Select where you want to see the notification label. The label can be displayed in all console sections, or in the **Monitoring & reporting** section and its subsections.

4. Click the **OK** button.

The Kaspersky announcement settings are specified.

## Disabling Kaspersky announcements

The [Kaspersky announcements](#) section (**Monitoring & reporting** → **Kaspersky announcements**) keeps you informed by providing information related to your version of Kaspersky Security Center Linux and managed applications installed on the managed devices. If you do not want to receive Kaspersky announcements, you can disable this feature.

The Kaspersky announcements include two types of information: security-related announcements and marketing announcements. You can disable the announcements of each type separately.

*To disable security-related announcements:*

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 **Kaspersky announcements** section.

3. Switch the toggle button to the **Security-related announcements are disabled** position.

4. Click the **Save** button.

Kaspersky announcements are disabled.

Marketing announcements are disabled by default. You receive marketing announcements only if you enabled Kaspersky Security Network (KSN). You can disable this type of announcement by disabling KSN.

To disable marketing announcements:

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 **KSN Proxy settings** section.
3. Disable the **Use Kaspersky Security Network Enabled** option.
4. Click the **Save** button.  
Marketing announcements are disabled.

## Exporting events to SIEM systems

This section describes how to configure export of events to the SIEM systems.

### Scenario: configuring event export to SIEM systems

Kaspersky Security Center Linux allows configuring event export to SIEM systems by one of the following methods: export to any SIEM system that uses Syslog format or export of events to SIEM systems directly from the Kaspersky Security Center database. When you complete this scenario, Administration Server sends events to a SIEM system automatically.

#### Prerequisites

Before you start configuration export of events in the Kaspersky Security Center Linux:

- [Learn more about the methods of event export.](#)
- Make sure that you have [the values of system settings](#).

You can perform the steps of this scenario in any order.

The process of export of events to a SIEM system consists of the following steps:

- **Configuring the SIEM system to receive events from Kaspersky Security Center Linux**

How-to instructions: [Configuring event export in a SIEM system](#)

- **Selecting the events that you want to export to the SIEM system**

Mark which events you want to export to the SIEM system. First, [mark the general events](#) that occur in all managed Kaspersky applications. Then, you can [mark the events for specific managed Kaspersky applications](#).

- **Configuring export of events to the SIEM system**

You can export events by using one of the following methods:

- [Using TCP/IP, UDP or TLS over TCP protocols](#)

- Using export of events directly [from the Kaspersky Security Center database](#) (a set of public views is provided in the Kaspersky Security Center database; you can find the description of these public views in the [klakdb.chm document](#))

## Results

After configuring export of events to a SIEM system you can view [export results](#) if you selected events which you want to export.

## Before you begin

When setting up automatic export of events in the Kaspersky Security Center Linux, you must specify some of the SIEM system settings. It is recommended that you check these settings in advance in order to prepare for setting up Kaspersky Security Center Linux.

To successfully configure automatic sending of events to a SIEM system, you must know the following settings:

- [SIEM system server address](#) 

The IP address of the server on which the currently used SIEM system is installed. Check this value in your SIEM system settings.

- [SIEM system server port](#) 

Port number used to establish a connection between Kaspersky Security Center Linux and your SIEM system server. You specify this value in the Kaspersky Security Center Linux settings and in the receiver settings of your SIEM system.

- [Protocol](#) 

Protocol used for transferring messages from Kaspersky Security Center Linux to your SIEM system. You specify this value in the Kaspersky Security Center Linux settings and in the receiver settings of your SIEM system.

## About event export

Kaspersky Security Center Linux allows you to receive information about [events](#) that occur during the operation of Administration Server and Kaspersky applications installed on managed devices. Information about events is saved in the Administration Server database.

You can use event export within centralized systems that deal with security issues on an organizational and technical level, provide security monitoring services, and consolidate information from different solutions. These are SIEM systems, which provide real-time analysis of security alerts and events generated by network hardware and applications, or Security Operation Centers (SOCs).



These systems receive data from many sources, including networks, security, servers, databases, and applications. SIEM systems also provide functionality to consolidate monitored data in order to help you avoid missing critical events. In addition, the systems perform automated analysis of correlated events and alerts in order to notify the administrators of immediate security issues. Alerting can be implemented through a dashboard or can be sent through third-party channels such as email.

The process of exporting events from Kaspersky Security Center Linux to external SIEM systems involves two parties: an event sender, Kaspersky Security Center Linux, and an event receiver, a SIEM system. To successfully export events, you must configure this in your SIEM system and in the Kaspersky Security Center Linux. It does not matter which side you configure first. You can either configure the transmission of events in the Kaspersky Security Center Linux, and then configure the receipt of events by the SIEM system, or vice versa.

## 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

The SIEM system must receive and correctly parse the events received from Kaspersky Security Center Linux. For these purposes, you must properly configure the SIEM system. The configuration depends on the specific SIEM system utilized. However, there are a number of general steps in the configuration of all SIEM systems, such as configuring the receiver and the parser.

## About configuring event export in a SIEM system

The process of exporting events from Kaspersky Security Center Linux to external SIEM systems involves two parties: an event sender—Kaspersky Security Center Linux and an event receiver—SIEM system. You must configure the export of events in your SIEM system and in the Kaspersky Security Center Linux.

The settings that you specify in the SIEM system depend on the particular system that you are using. Generally, for all SIEM systems you must set up a receiver and, optionally, a message parser to parse received events.

## Setting up the receiver

To receive events sent by Kaspersky Security Center Linux, you must set up the receiver in your SIEM system. In general, the following settings must be specified in the SIEM system:

- **Export protocol**

A message transfer protocol, either UDP, TCP, or TLS, over TCP. This protocol must be the same as the protocol you specified in Kaspersky Security Center Linux.

- **Port**

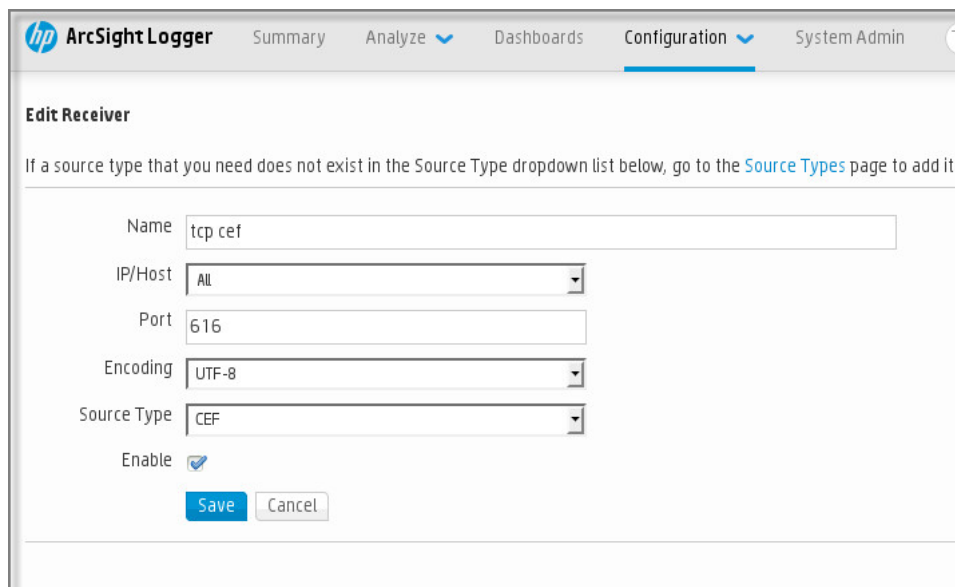
Specify the port number to connect to Kaspersky Security Center Linux. This port must be the same as [the port you specify in Kaspersky Security Center Linux during configuration with a SIEM system](#).

- **Data format**

Specify the Syslog format.

Depending on the SIEM system that you use, you may have to specify some additional receiver settings.

The figure below shows the receiver setup screen in ArcSight.



The screenshot displays the 'Edit Receiver' configuration page in the ArcSight web interface. The page title is 'hp ArcSight Logger' and the navigation menu includes 'Summary', 'Analyze', 'Dashboards', 'Configuration', and 'System Admin'. The main heading is 'Edit Receiver'. Below the heading, there is a note: 'If a source type that you need does not exist in the Source Type dropdown list below, go to the [Source Types](#) page to add it.' The configuration fields are: 'Name' (text input: tcp cef), 'IP/Host' (dropdown: All), 'Port' (text input: 616), 'Encoding' (dropdown: UTF-8), and 'Source Type' (dropdown: CEF). There is an 'Enable' checkbox with a checkmark. At the bottom, there are 'Save' and 'Cancel' buttons.

Receiver setup in ArcSight

## 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 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 Security Center Linux so that they can be stored in the SIEM system database.

## Marking of events for export to SIEM systems in Syslog format

This section describes how to mark events for further export to SIEM systems in Syslog format.

## About marking events for export to SIEM system in the 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 **Assets (Devices)** → **Policies & profiles**.
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 **Assets (Devices)** → **Managed devices**.  
The list of managed devices is displayed.
2. Click the link with the name of the required device in the list of managed devices.  
The properties window of the selected device is displayed.
3. Go to the **Applications** section.
4. Click the link with the name of the required application in the list of applications.
5. Go to the **Event configuration** section.
6. Select the check boxes next to the events that you want to export to SIEM.
7. Click the **Mark for export to SIEM system by using Syslog** button.

Also, you can mark an event for export to a SIEM system in the **Event registration** section, that 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 settings icon (⚙️) next to the name of the required Administration Server.
  - In the main menu, go to **Assets (Devices)** → **Policies & profiles**, 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**.

Also, you can mark an event for export to SIEM system in the **Event registration** section, that opens by clicking the link of the event.

4. A check mark (✓) appears in the **Syslog** column of the event or events that you marked for export to the SIEM system.

From now on, Administration Server sends the marked events to the SIEM system if export to the SIEM system is configured.

## About exporting events using Syslog format

You can use the Syslog format to export to SIEM systems the events that occur in Administration Server and other Kaspersky applications installed on managed devices.

Syslog is a standard for message logging protocol. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type that generates the message, and is assigned a severity level.

The Syslog format is defined by Request for Comments (RFC) documents published by the Internet Engineering Task Force (internet standards). The [RFC 5424](#) standard is used to export the events from Kaspersky Security Center Linux to external systems.

In Kaspersky Security Center Linux, you can configure export of the events to the external systems using the Syslog format.

The export process consists of two steps:

1. Enabling automatic event export. At this step, Kaspersky Security Center Linux is configured so that it sends events to the SIEM system. Kaspersky Security Center Linux starts sending events immediately after you enable automatic export.
2. Selecting the events to be exported to the external system. At this step, you select which event to export to the SIEM system.

## Configuring Kaspersky Security Center Linux for export of events to a SIEM system

To export events to a SIEM system, you have to configure the process of export in Kaspersky Security Center Linux.

*To configure export to SIEM systems in the Kaspersky Security Center Web Console:*

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 **SIEM** section.

3. Click the **Settings** link.

The **Export settings** section opens.

4. Specify the settings in the **Export settings** section:

- [SIEM system server address](#) ⓘ

The IP address of the server on which the currently used SIEM system is installed. Check this value in your SIEM system settings.

- [SIEM system port](#) ⓘ

Port number used to establish a connection between Kaspersky Security Center Linux and your SIEM system server. You specify this value in the Kaspersky Security Center Linux settings and in the receiver settings of your SIEM system.

- [Protocol](#) ⓘ

Select the protocol to be used for transferring messages to the SIEM system. You can select either the TCP/IP, UDP, or TLS over TCP protocol.

Specify the following TLS settings if you select the TLS over TCP protocol:

- **Server authentication**

In the **Server authentication** field, you can select the **Trusted certificates** or **SHA fingerprints** values:

- **Trusted certificates.** You can receive a file with the list of certificates from a trusted certification authority (CA) and upload the file to Kaspersky Security Center Linux. Kaspersky Security Center Linux checks whether the certificate of the SIEM system server is also signed by a trusted CA or not.

To add a trusted certificate, click the **Browse for CA certificates file** button, and then upload the certificate.

- **SHA fingerprints.** You can specify SHA-1 thumbprints of the SIEM system certificates in Kaspersky Security Center Linux. To add a SHA-1 thumbprint, enter it in the **Thumbprints** field, and then click the **Add** button.

By using the **Add client authentication** setting, you can generate a certificate to authenticate Kaspersky Security Center Linux. Thus, you will use a self-signed certificate issued by Kaspersky Security Center Linux. In this case, you can use both a trusted certificate and a SHA fingerprint to authenticate the SIEM system server.

- **Add Subject name/Subject alternative name**

Subject name is a domain name for which the certificate is received. Kaspersky Security Center Linux cannot connect to the SIEM system server if the domain name of the SIEM system server does not match the subject name of the SIEM system server certificate. However, the SIEM system server can change its domain name if the name has changed in the certificate. In this case, you can specify subject names in the **Add Subject name/Subject alternative name** field. If any of the specified subject names matches the subject name of the SIEM system certificate, Kaspersky Security Center Linux validates the SIEM system server certificate.

- **Add client authentication**

For client authentication, you can insert your certificate or generate it in Kaspersky Security Center Linux.

- **Insert certificate.** You can use a certificate that you received from any source, for example, from any trusted CA. You must specify the certificate and its private key by using one of the following certificate types:

- **X.509 certificate PEM.** Upload a file with a certificate in the **File with certificate** field, and a file with a private key in the **File with key** field. Both files do not depend on each other and the order of loading the files is not significant. When both files are uploaded, specify the password for decoding the private key in the **Password or certificate verification** field. The password can have an empty value if the private key is not encoded.
- **X.509 certificate PKCS12.** Upload a single file that contains a certificate and its private key in the **File with certificate** field. When the file is uploaded, specify the password for decoding the private key in the **Password or certificate verification** field. The password can have an empty value if the private key is not encoded.

- **Generate key.** You can generate a self-signed certificate in Kaspersky Security Center Linux. As a result, Kaspersky Security Center Linux stores the generated self-signed certificate, and you can pass the public part of the certificate or SHA1-fingerprint to the SIEM system.

5. If you want, you can export archived events from the Administration Server database and set the start date from which you want to start the export of archived events:
  - a. Click the **Set the export start date** link.
  - b. In the section that opens, specify the start date in the **Date to start export from** field.
  - c. Click the **OK** button.
6. Switch the option to the **Automatically export events to SIEM system database Enabled** position.
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.

## Exporting events directly from the database

You can retrieve events directly from the Kaspersky Security Center Linux database without having to use the Kaspersky Security Center Linux interface. You can either query the public views directly and retrieve the event data or create your own views on the basis of existing public views and address them to get the data you need.

### Public views

For your convenience, a set of public views is provided in the Kaspersky Security Center Linux database. You can find the description of these public views in the [klakdb.chm](#) document.

The `v_akpub_ev_event` public view contains a set of fields that represent the event parameters in the database. In the `klakdb.chm` document you can also find information on public views corresponding to other Kaspersky Security Center Linux entities, for example, devices, applications, or users. You can use this information in your queries.

This section contains instructions for creating an SQL query by means of the `klsq12` utility and a query example.

To create SQL queries or database views, you can also use any other program for working with databases. Information on how to view the parameters for connecting to the Kaspersky Security Center Linux database, such as instance name and database name, is given in the corresponding section.

## Creating an SQL query using the `klsq12` utility

This section describes how to use the `klsq12` utility, and create an SQL query by using this utility. Use `klsq12` utility version that is included in your Kaspersky Security Center Linux version installed.

*To use the `klsq12` utility:*

1. Go to /opt/kaspersky/ksc64/sbin/klsq12 directory on the device with Kaspersky Security Center Administration Server installed.
2. In this directory, create src.sql blank file.
3. Open the src.sql file in any text editor.
4. In the src.sql file, type the SQL query that you want, and then save the file.
5. On the device with Kaspersky Security Center Administration Server installed, in the command line, type the following command to run the SQL query from the src.sql file and save the results to the result.xml file:  

```
sudo ./klsq12 -i src.sql -u <username> -p <password> -o result.xml
```

 where <username> and <password> are credentials of the user account that has access to the database.
6. If required, enter the login and password of the user account that has access to the database.
7. Open the newly created result.xml file to view the query results.

You can edit the src.sql file and create any query to the public views. Then, from the command line, execute your query and save the results to a file.

## Example of an SQL query in the klsq12 utility

This section shows an example of an SQL query, created by means of the klsq12 utility.

The following example illustrates retrieval of the events that occurred on devices during the last seven days, and display of the events ordered by the time they occur, the most recent events are displayed first.

### Example:

```
SELECT
 e.nId, /* event identifier */
 e.tmRiseTime, /* time, when the event occurred */
 e.strEventType, /* internal name of the event type */
 e.wstrEventTypeDisplayName, /* displayed name of the event */
 e.wstrDescription, /* displayed description of the event */
 e.wstrGroupName, /* name of the group, where the device is located */
 h.wstrDisplayName, /* displayed name of the device, on which the event occurred */
 CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
 CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
 CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
 CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* IP-address of the device, on which
 the event occurred */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

## Viewing the Kaspersky Security Center Linux database name



If you want to access Kaspersky Security Center Linux database by means of the SQL Server, MySQL, or MariaDB database management tools, you must know the name of the database in order to connect to it from your SQL script editor.

To view the name of the Kaspersky Security Center Linux database:

1. In the main menu, click the settings icon (⚙️) next to the name of the required Administration Server.  
The Administration Server properties window opens.

2. On the **General** tab, select the **Details of current database** section.

The database name is specified in the **Database name** field. Use the database name to address the database in your SQL queries.

## Viewing export results

You can control for successful completion of the event export procedure. To do this, check whether messages with export events are received by your SIEM system.

If the events sent from Kaspersky Security Center Linux are received and properly parsed by your SIEM system, configuration on both sides is done properly. Otherwise, check the settings you specified in Kaspersky Security Center Linux against the configuration in your SIEM system.

The figure below shows the events exported to ArcSight. For example, the first event is a critical Administration Server event: "Device status is Critical".

The representation of export events in the SIEM system varies according to the SIEM system you use.

| Time (Event Time)         | Device                          | Logger | deviceVendor | deviceProduct  | deviceVersion |
|---------------------------|---------------------------------|--------|--------------|----------------|---------------|
| 1 2017/01/24 17:27:11 MSK | mikrotik_admin.avp.ru [tcp cef] | Local  | KasperskyLab | SecurityCenter | 10.4.343      |
| 2 2017/01/24 17:26:41 MSK | mikrotik_admin.avp.ru [tcp cef] | Local  | KasperskyLab | SecurityCenter | 10.4.343      |

Example of events

## Managing object revisions

This section contains information about object revision management. Kaspersky Security Center Linux allows you to track object modification. Every time you save changes made to an object, a *revision* is created. Each revision has a number.

Application objects that support revision management include:

- Administration Servers
- Policies
- Tasks
- Administration groups
- User accounts
- Installation packages

You can perform the following actions on object revisions:

- Compare a selected revision to the current one
- Compare selected revisions
- Compare an object to a selected revision of another object of the same type
- View a selected revision
- Roll back changes made to an object to a selected revision
- Save revisions as a .txt file

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:

- Object revision number
- Date and time the object was modified
- Name of the user who modified the object
- Action performed on the object
- 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 **Description** button. In the **Object revision description** window, enter some text for the revision description.

## About object revisions

You can perform the following actions on object revisions:

- Compare a selected revision to the current one

- Compare selected revisions
- Compare an object to a selected revision of another object of the same type
- View a selected revision
- Roll back changes made to an object to a selected revision
- Save revisions as a .txt file

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:

- Object revision number
- Date and time the object was modified
- Name of the user who modified the object
- Action performed on the object
- Description of the revision related to the change made to the object settings

## Rolling back an object to a previous revision

You can roll back changes made to an object, if necessary. For example, you may have to revert the settings of a policy to their state on a specific date.

*To roll back changes made to an object:*

1. In the object's properties window, open the **Revision history** tab.
2. In the list of object revisions, select the revision that you want to roll back changes for.
3. Click the **Roll back** button.
4. Click **OK** to confirm the operation.

The object is now rolled back to the selected revision. The list of object revisions displays a record of the action that was taken. The revision description displays information about the number of the revision to which you reverted the object.

Rolling back operation is available only for policy and task objects.

## Deletion of objects

This section provides information about deleting objects and viewing information about objects after they are deleted.

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 Security Center Linux handles the devices in the Unassigned devices group according to the following rules:

- If you have configured [device moving rules](#) and a device meets the criteria of a moving rule, the device is automatically moved to an administration group according to the rule.
- The device is stored in the Unassigned devices group and automatically removed from the group according to the device retention rules.

The device retention rules do not affect the devices that have one or more drives encrypted with [full disk encryption](#). Such devices are not deleted automatically—you can only delete them manually. If you need to delete a device with an encrypted drive, first decrypt the drive, and then delete the device.

When you delete a device with encrypted drive, the data required to decrypt the drive is also deleted. In this case, to decrypt the drive, the following conditions must be met:

- The device is reconnected to Administration Server to restore the data required to decrypt the drive.
- The device user remembers the decryption password.
- The security application that was used to encrypt the drive, for example Kaspersky Endpoint Security for Windows, is still installed on the device.

If the drive was encrypted by Kaspersky Disk Encryption technology, you can also try [recovering data by using the FDERT Restore Utility](#)<sup>2</sup>.

When you delete a device from the Unassigned devices group manually, the application removes the device from the list. After device deletion, the installed Kaspersky applications (if any) remain on the device. Then, if the device is still visible to Administration Server and you have configured regular network polling, Kaspersky Security Center Linux discovers the device during the network polling and adds it back to the Unassigned devices group. Therefore, it is reasonable to delete a device manually only if the device is invisible to Administration Server.

## Downloading and deleting files from Quarantine and Backup

This section gives information on how to download and how to delete files from Quarantine and Backup in Kaspersky Security Center Web Console.

### Downloading files from Quarantine and Backup

You can download files from Quarantine and Backup only if one of the two conditions is met: either the **Do not disconnect from the Administration Server** option is enabled in the settings of the device, or a connection gateway is in use. Otherwise, the downloading is not possible.

*To save a copy of file from Quarantine or Backup to a hard drive:*

1. Do one of the following:

- If you want to save a copy of file from Quarantine, in the main menu, go to **Operations** → **Repositories** → **Quarantine**.
- If you want to save a copy of file from Backup, in the main menu, go to **Operations** → **Repositories** → **Backup**.

2. In the window that opens, select a file that you want to download and click **Download**.

The download starts. A copy of the file that had been placed in Quarantine on the client device is saved to the specified folder.

### About removing objects from the Quarantine, Backup, or Active threats repositories

When Kaspersky security applications installed on client devices place objects to the Quarantine, Backup, or Active threats repositories, they send the information about the added objects to the **Quarantine**, **Backup**, or **Active threats** sections in Kaspersky Security Center Linux. When you open one of these sections, select an object from the list and click the **Remove** button, Kaspersky Security Center Linux performs one of the following actions or both actions:

- Removes the selected object from the list
- Deletes the selected object from the repository

The action to perform is defined by the Kaspersky application that placed the selected object to the repository. The Kaspersky application is specified in the **Entry added by** field. Refer to the documentation of the Kaspersky application for details about which action is to be performed.

## 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 **Assets (Devices) → Managed 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. In the window that opens, click **Remote diagnostics**.

This opens the **Remote diagnostics** window of a client device. If connection between Administration Server and the client device is not established, the error message displays.

Alternatively, if you need to obtain all diagnostic information about a Linux-based client device at once, you can [run the collect.sh script](#) on this device.

## Enabling and disabling tracing for applications

You can enable and disable tracing for applications, including Xperf tracing.

## Enabling and disabling tracing

To enable or disable tracing on a remote device:

1. [Open the remote diagnostics window of a client device.](#)
2. In the remote diagnostics window, select the **Kaspersky applications** tab.  
In the **Application management** section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select the application for which you want to enable or disable tracing.  
The list of remote diagnostics options opens.
4. If you want to enable tracing:

a. In the **Tracing** section, click **Enable tracing**.

b. In the **Modify tracing level** window that opens, we recommend that you keep the default values of the settings. When required, a Technical Support specialist will guide you through the configuration process. The following settings 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 **Save**.

The tracing is enabled for the selected application. In some cases, the security application and its task must be restarted in order to enable tracing.

On Linux-based client devices, tracing for the Updater of Network Agent component is regulated by the Network Agent settings. Therefore, the **Enable tracing** and **Modify tracing level** options are disabled for this component on client devices running Linux.

5. If you want to disable tracing for the selected application, click the **Disable tracing** button.

The tracing is disabled for the selected application.

## Enabling Xperf tracing

For Kaspersky Endpoint Security, a Technical Support specialist may ask you to enable Xperf tracing for information about the system performance.

To enable and configure Xperf tracing or disable it:

1. [Open the remote diagnostics window of a client device.](#)

2. In the remote diagnostics window, select the **Kaspersky applications** tab.

In the **Application management** section, the list of Kaspersky applications installed on the device displays.

3. In the list of applications, select Kaspersky Endpoint Security for Windows.

The list of remote diagnostics options for Kaspersky Endpoint Security for Windows displays.

4. In the **Xperf tracing** section, click **Enable Xperf tracing**.

If Xperf tracing is already enabled, the **Disable Xperf tracing** button is displayed instead. Click this button if you want to disable Xperf tracing for Kaspersky Endpoint Security for Windows.

5. In the **Change Xperf tracing level** window that opens, depending on the request from the Technical Support specialist, do the following:

a. Select one of the following tracing levels:

- [Light level](#) 

A trace file of this type contains the minimum amount of information about the system.  
By default, this option is selected.

- [Deep level](#) 

A trace file of this type contains more detailed information than trace files of the *Light* type and may be requested by Technical Support specialists when a trace file of the *Light* type is not enough for the performance evaluation. A *Deep* trace file contains technical information about the system including information about hardware, operating system, list of started and finished processes and applications, events used for performance evaluation, and events from Windows System Assessment Tool.

b. Select one of the following Xperf tracing types:

- [Basic type](#) 

The tracing information is received during operation of the Kaspersky Endpoint Security application.  
By default, this option is selected.

- [On-restart type](#) 

The tracing information is received when the operating system starts on the managed device. This tracing type is effective when the issue that affects the system performance occurs after the device is turned on and before Kaspersky Endpoint Security starts.

You may also be asked to enable the **Rotation file size, in MB** option to prevent excessive increase in the size of the trace file. Then specify the maximum size of the trace file. When the file reaches the maximum size, the oldest tracing information is overwritten with new information.

c. Define the rotation file size.

d. Click **Save**.



Xperf tracing is enabled and configured.

6. If you want to disable Xperf tracing for Kaspersky Endpoint Security for Windows, click **Disable Xperf tracing** in the **Xperf tracing** section.

Xperf tracing is disabled.

## Downloading trace files of an application

*To download a trace file of an application:*

1. [Open the remote diagnostics window of a client device.](#)
2. In the remote diagnostics window, select the **Kaspersky applications** tab.  
In the **Application management** section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select the application for which you want to download a trace file.
4. In the **Tracing** section, click the **Trace files** button.  
This opens the **Device tracing logs** window, where a list of trace files is displayed.
5. In the list of trace files, select the file that you want to download.
6. Do one of the following:
  - Download the selected file by clicking **Download**. You can select one or several files for downloading.
  - Download a portion of the selected file:
    - a. Click **Download a portion**.  
You cannot download portions of several files at the same time. If you select more than one trace file, the **Download a portion** button will be disabled.
    - b. In the window that opens, specify the name and the file portion to download, according to your needs.  
For Linux-based devices, editing the file portion name is not available.
    - c. Click **Download**.

The selected file, or its portion, is downloaded to the location that you specify.

## Deleting trace files

You can delete trace files that are no longer needed.

*To delete a trace file:*

1. [Open the remote diagnostics window of a client device.](#)
2. In the remote diagnostics window that opens, select the **Event logs** tab.

3. In the **Trace files** section, click **Windows Update logs** or **Remote installation logs**, depending on which trace files you want to delete.

The **Windows Update logs** link is available only for Windows-based client devices.

This opens the **Device tracing logs** window, where a list of trace files is displayed.

4. In the list of trace files, select one or several files that you want to delete.
5. Click the **Remove** button.

The selected trace files are deleted.

## Downloading application settings

*To download application settings from a client device:*

1. [Open the remote diagnostics window of a client device.](#)
2. In the remote diagnostics window, select the **Kaspersky applications** tab.
3. In the **Application settings** section, click the **Download** button to download information about the settings of the applications installed on the client device.

The ZIP archive with information is downloaded to the specified location.

## Downloading system information from a client device

*To download system information from a client device:*

1. [Open the remote diagnostics window of a client device.](#)
2. In the remote diagnostics window, select the **System information** tab.
3. Click the **Download** button to download the system information about the client device.

If you obtain system information about a Linux-based device, a dump file for emergency terminated applications is added to the resulting file.

The file with information is downloaded to the specified location.

## Downloading event logs

*To download an event log from a remote device:*

1. [Open the remote diagnostics window of a client device.](#)
2. In the remote diagnostics window, on the **Event logs** tab, click **All device logs**.

3. In the **All device logs** window, select one or several relevant logs.

4. Do one of the following:

- Download the selected log by clicking **Download entire file**.
- Download a portion of the selected log:
  - a. Click **Download a portion**.

You cannot download portions of several logs at the same time. If you select more than one event log, the **Download a portion** button will be disabled.
  - b. In the window that opens, specify the name and the log portion to download, according to your needs.

For Linux-based devices, editing the log portion name is not available.
  - c. Click **Download**.

The selected event log, or a portion of it, is downloaded to the specified location.

## Starting, stopping, restarting the application

You can start, stop, and restart applications on a client device.

*To start, stop, or restart an application:*

1. [Open the remote diagnostics window of a client device](#).
2. In the remote diagnostics window, select the **Kaspersky applications** tab.

In the **Application management** section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select the application that you want to start, stop, or restart.
4. Select an action by clicking one of the following buttons:
  - **Stop application**

This button is available only if the application is currently running.
  - **Restart application**

This button is available only if the application is currently running.
  - **Start application**

This button is available only if the application is not currently running.

Depending on the action that you have selected, the required application is started, stopped, or restarted on the client device.

If you restart the Network Agent, a message is displayed stating that the current connection of the device to the Administration Server will be lost.

## Running the remote diagnostics of Kaspersky Security Center Linux Network Agent and downloading the results

To start diagnostics for Kaspersky Security Center Linux Network Agent on a remote device and download the results:

1. [Open the remote diagnostics window of a client device.](#)
2. In the remote diagnostics window, select the **Kaspersky applications** tab.  
In the **Application management** section, the list of Kaspersky applications installed on the device displays.
3. In the list of applications, select **Kaspersky Security Center Linux Network Agent**.  
The list of remote diagnostics options opens.
4. In the **Diagnostics report** section, click the **Run diagnostics** button.  
This starts the remote diagnostics process and generates a diagnostics report. When the diagnostics process is complete, the **Download diagnostics report** button becomes available.
5. Click the **Download diagnostics report** button to download the report.  
The report is downloaded to the specified location.

## Running an application on a client device

You may have to run an application on the client device, if a Kaspersky support specialist requests it. You do not have to install the application on that device.

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 **Application files** section, click the **Browse** button to select a ZIP archive containing the application that you want to run on the client device.

The ZIP archive must include the utility folder. This folder contains the executable file to be run on a remote device.

You can specify the executable file name and the command-line arguments, if necessary. To do this, fill in the **Executable file in an archive to be run on a remote device** and **Command-line arguments** fields.

4. Click the **Upload and run** button to run the specified application on a client device.
5. Follow the instructions of the Kaspersky support specialist.

## Generating a dump file for an application

An application dump file allows you to view 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 click 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 Security Center Linux allows you to [download the basic diagnostic information from a client device](#). Alternatively, you can obtain the diagnostic information about a Linux-based device by using the collect.sh script by Kaspersky. This script is run on the Linux-based client device that needs to be diagnosed, and then it generates a file with the diagnostic information, the system information about this device, trace files of applications, device logs, and a dump file for emergency-terminated applications.

We recommend that you use the collect.sh script to obtain all diagnostic information about the Linux-based client device at once. If you download the diagnostic information remotely through Kaspersky Security Center Linux, you will need to go through all sections of the [remote diagnostics interface](#). Also the diagnostic information for a Linux-based device will probably not be obtained completely.

If you need to send the generated file with the diagnostic information to the Kaspersky Technical Support, delete all confidential information before sending the file.

*To download the diagnostic information from a Linux-based client device by using the collect.sh script:*

1. [Download the collect.sh script](#)  packed in the collect.tar.gz archive.
2. Copy the downloaded archive to the Linux-based client device that needs to be diagnosed.

3. Run the following command to unpack the collect.tar.gz archive:

```
tar -xzf collect.tar.gz
```

4. Run the following command to specify the script execution rights:

```
chmod +x collect.sh
```

5. Run the collect.sh script by using an account with administrator rights:

```
./collect.sh
```

A file with the diagnostic information is generated and saved to the /tmp/\$HOST\_NAME-collect.tar.gz folder.

# Managing third-party applications on client devices

This section describes the features of Kaspersky Security Center Linux related to the management of third-party applications run on client devices.

## Scenario: Application Management

You can manage applications startup on user devices. You can allow or block applications to be run on managed devices. This functionality is realized by the Application Control component. You can manage applications installed on Windows or Linux devices.

For Linux-based operating systems, Application Control component is available starting from Kaspersky Endpoint Security 11.2 for Linux.

### Prerequisites

- Kaspersky Security Center Linux is deployed in your organization.
- The policy of Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Windows is created and is active.

### Stages

The Application Control usage scenario proceeds in stages:

#### 1 Forming and viewing the list of applications on client devices

This stage helps you find out what applications are installed on managed devices. You can view the list of applications and decide which applications you want to allow and which you want to prohibit, according to your organization's security policies. The restrictions can be related to the information security policies in your organization. You can skip this stage if you know exactly what applications are installed on managed devices.

How-to instructions: [Obtaining and viewing a list of applications installed on client devices](#)

#### 2 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 policies in your organization. You can skip this stage if you know exactly what executable files are installed on managed devices.

How-to instructions: [Obtaining and viewing a list of executable files stored on client devices](#)

#### 3 Creating application categories for the applications used in your organization

Analyze the lists of applications and executable files stored on managed devices. Basing on the analysis, create application categories. It is recommended to create a "Work applications" category that covers the standard set of applications that are used at your organization. If different security groups use different sets of applications in their work, a separate application category can be created for each security group.

Depending the set of criteria to create an application category, you can create application categories of two types.

How-to instructions: [Creating application category with content added manually](#), [Creating application category that includes executable files from selected devices](#)

#### 4 Configuring Application Control in the Kaspersky Endpoint Security policy

Configure the Application Control component in Kaspersky Endpoint Security for Linux policy using the application categories you have created on the previous stage.

How-to instructions: [Configuring Application Control in the Kaspersky Endpoint Security for Windows policy](#)

#### 5 Turning on Application Control component in test mode

To ensure that Application Control rules do not block applications 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 applications whose startup is forbidden by Application Control rules, but will instead send notifications about their startup to the Administration Server.

When testing Application Control rules, it is recommended to perform the following actions:

- Determine the testing period. Testing period can vary from several days to two months.
- Examine the events resulting from testing the operation of Application Control.

How-to instructions for Kaspersky Security Center Web Console: [Configuring Application Control component in the Kaspersky Endpoint Security for Windows policy](#). Follow this instruction and enable the **Test Mode** option in configuration process.

#### 6 Changing the application 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: Kaspersky Security Center Web Console: [Adding event-related executable files to the application category](#)

#### 7 Applying the rules of Application Control in operation mode

After Application Control rules are tested and configuration of application categories is complete, you can apply the rules of Application Control in operation mode.

How-to instructions for Kaspersky Security Center Web Console: [Configuring Application Control component in the Kaspersky Endpoint Security for Windows policy](#). Follow this instruction and disable the **Test Mode** option in configuration process.

#### 8 Verifying Application Control configuration

Be sure that you have done the following:

- Created application categories.
- Configured Application Control using the application categories.
- Applied the rules of Application Control in operation mode.

## Results

When the scenario is complete, applications startup on managed devices is controlled. The users can start only those applications that are allowed in your organization and cannot start applications that are prohibited in your organization.

For detailed information about Application Control, refer to the [Kaspersky Endpoint Security for Linux Help](#) and [Kaspersky Endpoint Security for Windows Help](#).

## About Application Control

The Application Control component monitors users' attempts to start applications and regulates the startup of applications by using Application Control rules.

Application Control component is available for Kaspersky Endpoint Security 11.2 for Linux and later versions.

Startup of applications 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 applications except the applications specified in block rules. This mode is selected by default.
- *Allowlist*. The mode is used if you want to block the startup of all applications except the applications specified in allow rules.

The Application Control rules are implemented through application categories. You create application categories defining specific criteria. In Kaspersky Security Center Linux there are three types of application categories:

- [Category with content added manually](#). You define conditions, for example, file metadata, file hashcode, file certificate, file path, to include executable files in the category.
- [Category that includes executable files from selected devices](#). You specify a device whose executable files are automatically included in the category.
- [Category that includes executable files from selected folder](#). You specify a folder from which executable files are automatically included in the category.

For detailed information about Application Control, refer to the [Kaspersky Endpoint Security for Linux Help](#) and [Kaspersky Endpoint Security for Windows Help](#).

## Obtaining and viewing a list of applications installed on client devices

Kaspersky Security Center Linux inventories all software installed on managed client devices running Linux and Windows.

Network Agent compiles a list of applications installed on a device, and then transmits this list to Administration Server. It takes about 10-15 minutes for the Network Agent to update the application list.

For Windows-based client devices, Network Agent receives most of the information about installed applications from the Windows registry. For Linux-based client devices, package managers provide information about installed applications to Network Agent.



*To view the list of applications installed on managed devices:*

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



2. You can group and filter the data of the table with installed applications as follows:

- Click the settings icon (  ) in the upper-right corner of the table.  
In the invoked **Columns settings** menu, select the columns to be displayed in the table. To view the operating system type of the client devices on which the application is installed, select the **Operating system 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 **Devices** → **Managed devices** → **<device name>** → **Advanced** → **Applications registry**. In this menu, you can export the list of applications to a CSV file or TXT file.

For detailed information about Application Control, refer to the [Kaspersky Endpoint Security for Linux Help](#) and [Kaspersky Endpoint Security for Windows Help](#).

## Obtaining and viewing a list of executable files stored on client devices

You can obtain a list of executable files stored on managed devices. To inventory executable files, you must create an inventory task.

For Kaspersky Endpoint Security for Linux, the feature of inventorying executable files is available since no earlier than version 11.2.

*To create an inventory task for executable files on client devices:*

1. In the main menu, go to **Assets (Devices)** → **Tasks**.  
The list of tasks is displayed.
2. Click the **Add** button.  
The [New task wizard](#) starts. Follow the steps of the wizard.
3. On the **New task** page, from the **Application** drop-down list, select Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Windows, depending on the operating system of the client devices.
4. From the **Task type** drop-down list, select **Inventory**.
5. On the **Finish task creation** page, click the **Finish** button.

After the New task wizard has finished, the **Inventory** task is created and configured. If you want, you can change the settings for the created task. The newly created task is displayed in the list of tasks.

For a detailed description of the inventory task, see the [Kaspersky Endpoint Security for Linux Help](#) and the [Kaspersky Endpoint Security for Windows Help](#).

After the **Inventory** task is performed, the list of executable files stored on managed devices is formed, and you can view the list.

During inventory, executable files in the following formats are detected: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, and HTML.

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 stored on client devices.

## 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. Follow the steps of the wizard.

3. On the **Select category creation method** page of the wizard, specify the application category name and select the **Category with content added manually. Data of executable files is manually added to the category** option.

4. On the **Conditions** page of the wizard, click the **Add** button to add a condition criterion to include files in the creating category.

5. On the **Condition criteria** page, 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 storage. Executable files that have been signed in accordance with the specified certificates will be added to the user category.

- [Specify path to application \(masks supported\)](#) 

If this option is selected, you can specify the path to the folder on the client device containing the executable files that are to be added to the user application category.

- [Removable drive](#) 

If this option is selected, you can specify the type of the medium (any drive or removable drive) on which the application is run. Applications that have been run on the selected drive type are added to the user application category.

- Hash, metadata, or certificate:

- [Select from list of executable files](#) 

If this option is selected, you can use the list of executable files on the client device to select and add applications to the category.

- [Select from applications registry](#) 

If this option is selected, application registry is displayed. You can select an application from the registry and specify the following file metadata:

- File name.
- 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.

- [Specify manually](#) 

If this option is selected, you must specify file hash, or metadata, or certificate as the condition of adding applications to the user category.

### File Hash

Depending on the version of the security application installed on devices on your network, you should select an algorithm for hash value computing by Kaspersky Security Center Linux for files in this category. Information about computed hash values is stored in the Administration Server database. Storage of hash values does not increase the database size significantly.

SHA-256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security for Linux supports SHA-256 computing.

Select either of the options of hash value computing by Kaspersky Security Center Linux for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security for Linux, select the **SHA-256** check box.
- Select the **MD5 hash** check box only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support the MD5 hash function.

### Metadata

If this option is selected, you can specify file metadata as file name, file version, vendor. The metadata will be sent to Administration Server. Executable files that contain the same metadata will be added to the application category.

### Certificate

If this option is selected, you can specify certificates from the storage. Executable files that have been signed in accordance with the specified certificates will be added to the user category.

- [From archived folder](#) 

If this option is selected, you can specify a file of an archived folder, and then select which condition you want to use to add applications to the user category. The archived folder is unpacked and the conditions that you select are applied to the files in the folder. As a condition, you can select one of the following criteria:

- **File Hash**

You select which hash function (MD5 or SHA-256) you want to use to calculate hash values. The applications that have the same hash value as the files in the archived folder are added to the user application category.

Select an MD5 hash function only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support the MD5 hash function.

- **Metadata**

You select which metadata you want to use as criteria. Executable files that contain the same metadata will be added to the user application category.

- **Certificate**

You select which certificate properties (certificate subject, fingerprint, or issuer) you want to use as criteria. Executable files that have been signed with the certificates that have the same properties will be added to the user category.

If this option is selected, you can specify a file of an archived folder, and then select which condition you want to use to add applications to the user category. The archived folder is unpacked and the conditions that you select are applied to the files in the folder. As a condition, you can select one of the following criteria:

- **File Hash**

You select which hash function (MD5 or SHA-256) you want to use to calculate hash values. The applications that have the same hash value as the files in the archived folder are added to the user application category.

Select an MD5 hash function only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support the MD5 hash function.

- **Metadata**

You select which metadata you want to use as criteria. Executable files that contain the same metadata will be added to the user application category.

- **Certificate**

You select which certificate properties (certificate subject, fingerprint, or issuer) you want to use as criteria. Executable files that have been signed with the certificates that have the same properties will be added to the user category.

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** page of the wizard, click the **Add** button to add an exclusive condition criterion to exclude files from the category that is being created.

7. On the **Condition criteria** page, 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 [Kaspersky Endpoint Security for Linux Help](#) and [Kaspersky Endpoint Security for Windows Help](#).

## Creating an application category that includes executable files from selected devices

You can use executable files from selected devices as a template of executable files that you want to allow or block. Based on executable files from selected devices, you can create an application category and use it in the Application Control component configuration.

*To create application 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 application categories is displayed.

2. Click the **Add** button.

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

3. On the **Select category creation method** page of the wizard, 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 application category.
6. Specify the following settings:

- [Hash value computing algorithm](#)

Depending on the version of the security application installed on devices on your network, you should select an algorithm for hash value computing by Kaspersky Security Center Linux for files in this category. Information about computed hash values is stored in the Administration Server database. Storage of hash values does not increase the database size significantly.

SHA-256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security for Linux supports SHA-256 computing.

Select either of the options of hash value computing by Kaspersky Security Center Linux for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security for Linux, select the **SHA-256** check box.

Select the **MD5 hash** check box only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support the MD5 hash function.

The **Calculate SHA-256 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 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.

## Creating an application category that includes executable files from selected folder

You can use executable files from a selected folder as a standard of executable files that you want to allow or block in your organization. On the basis of executable files from the selected folder, you can create an application category and use it in the Application Control component configuration.

*To create an application category that includes executable files from the selected folder:*

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** page of the wizard, specify the category name and select the **Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category** option.

4. Specify the folder whose executable files will be used to create the application category.

5. Define the following settings:

- [Include dynamic-link libraries \(DLL\) in this category](#) 

The application category includes dynamic-link libraries (files in DLL format), and the Application Control component logs the actions of such libraries running in the system. Including DLL files in the category may lower the performance of Kaspersky Security Center.

By default, this check box is cleared.

- [Include script data in this category](#) 

The application category includes data on scripts, and scripts are not blocked by Web Threat Protection. Including the script data in the category may lower the performance of Kaspersky Security Center.

By default, this check box is cleared.

- [Hash value computing algorithm](#): Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions) / Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)

Depending on the version of the security application installed on devices on your network, you should select an algorithm for hash value computing by Kaspersky Security Center Linux for files in this category. Information about computed hash values is stored in the Administration Server database. Storage of hash values does not increase the database size significantly.

SHA-256 is a cryptographic hash function: no vulnerabilities have been found in its algorithm, and so it is considered the most reliable cryptographic function nowadays. Kaspersky Endpoint Security for Linux supports SHA-256 computing.

Select either of the options of hash value computing by Kaspersky Security Center Linux for files in the category:

- If all instances of security applications installed on your network are Kaspersky Endpoint Security for Linux, select the **SHA-256** check box.

Select the **MD5 hash** check box only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support the MD5 hash function.

The **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)** check box is selected by default.

The **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** is cleared by default.

- [Force folder scan for changes](#)

If this option is enabled, the application regularly checks the folder of category content addition for changes. You can specify the frequency of checks (in hours) in the entry field next to the check box. By default, the time interval between forced checks is 24 hours.

If this option is disabled, the application does not force any checks of the folder. The Server attempts to access files if they have been modified, added, or deleted.

By default, this option is disabled.

When the wizard finishes, the application category is created. It is displayed in the list of application categories. You can use the application category at Application Control configuration.

For detailed information about Application Control, refer to the [Kaspersky Endpoint Security for Linux Help](#) and [Kaspersky Endpoint Security for Windows Help](#).

## Viewing the list of application categories

You can view the list of configured 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 **Assets (Devices)** → **Policies & profiles**.

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 computer after selecting the **Control DLL modules load** option if you want Kaspersky Endpoint Security for Windows to monitor all DLL modules and drivers, including those loaded before Kaspersky Endpoint Security for Windows is started.

7. (Optional) In the **Message templates** block, change the template of the message that is displayed when an application is blocked from starting and the template of the email message that is sent to you.

8. In the **Application Control Mode** block settings, select the **Denylist** or **Allowlist** mode.

By default, the **Denylist** mode is selected.

9. Click the **Rules Lists Settings** link.

The **Denylists and allowlists** window opens to let you add an application category. By default, the **Denylist** tab is selected if the **Denylist** mode is selected, and the **Allowlist** tab is selected if the **Allowlist** mode is selected.

10. In the **Denylists and allowlists** window, click the **Add** button.

The **Application Control rule** window opens.

11. Click the **Please choose a category** link.

The **Application Category** window opens.

12. Add the application category (or categories) that you created earlier.

You can edit the settings of a created category by clicking the **Edit** button.

You can create a new category by clicking the **Add** button.

You can delete a category from the list by clicking the **Delete** button.

13. After the list of application categories is complete, click the **OK** button.

The **Application Category** window closes.

14. In the **Application Control** rule window, in the **Subjects and their rights** section, create a list of users and groups of users to apply the Application Control rule.

15. Click the **OK** button to save the settings and to close the **Application Control rule** window.

16. Click the **OK** button to save the settings and to close the **Denylists and allowlists** window.

17. Click the **OK** button to save the settings and to close the **Application Control** window.

18. Close the window with the Kaspersky Endpoint Security for Windows policy settings.

Application Control is configured. After the policy is propagated to the client devices, the startup of executable files is managed.

For detailed information about Application Control, refer to the [Kaspersky Endpoint Security for Linux Help](#) and [Kaspersky Endpoint Security for Windows Help](#).

## Adding event-related executable files to the application category

After you configure Application Control in the Kaspersky Endpoint Security policies, the following events will be displayed in the list of events:

- **Application startup prohibited** (*Critical* event). This event is displayed if you have configured Application Control to apply rules.
- **Application startup prohibited in test mode** (*Info* event). This event is displayed if you have configured Application Control to test rules.
- **Message to administrator about application startup prohibition** (*Warning* event). This event is displayed if you have configured Application Control to apply rules and a user has requested access to the application that is blocked at startup.

It is recommended to [create event selections](#) to view events related to Application Control operation.

You can add executable files related to Application Control events to an existing application category or to a new application category. You can add executable files only to an application category with content added manually.

To add executable files related to Application Control events to an application category:

1. In the main menu, go to **Monitoring & reporting** → **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 \(or SHA-256 hashes for files without a certificate\)](#) ⓘ

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 SHA-256 (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)** [?](#)

Select this option only if you use Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux does not support an MD5 hash function.

Each file has its own unique MD5 hash function. When you select an MD5 hash function, only one corresponding file, for example, the defined application version, ends up in the category.

5. Click **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 [Kaspersky Endpoint Security for Linux Help](#) and [Kaspersky Endpoint Security for Windows Help](#).

# Sizing Guide

This section provides information about Kaspersky Security Center Linux sizing.

## About this Guide

Kaspersky Security Center Linux (also referred to as Kaspersky Security Center) Sizing Guide is intended for professionals who install and administer Kaspersky Security Center, as well as for those who provide technical support to organizations that use Kaspersky Security Center.

All recommendations and calculations are given for networks on which Kaspersky Security Center manages the protection of devices with Kaspersky software installed.

To obtain and maintain optimum performance under varying operational conditions, you must take into account the number of networked devices, network topology, and set of Kaspersky Security Center features that you require.

This Guide provides the following information:

- Limitations of Kaspersky Security Center
- Calculations for the key nodes of Kaspersky Security Center (Administration Servers and distribution points):
  - Hardware requirements for Administration Servers and distribution points
  - Calculation of the number and hierarchy of Administration Servers
  - Calculation of the number and configuration of distribution points
- Configuration of event logging in the database depending on the number of networked devices
- Configuration of specific tasks aimed at optimal performance of Kaspersky Security Center
- Traffic rate (network load) between Kaspersky Security Center Administration Server and every protected device

Consulting this guide is recommended in the following cases:

- When planning resources prior to Kaspersky Security Center installation
- When planning significant changes to the scale of the network on which Kaspersky Security Center is deployed
- When switching from using Kaspersky Security Center within a limited network segment (a test environment) to full-scale deployment of Kaspersky Security Center on the corporate network
- When making changes to the set of Kaspersky Security Center features used

## Calculations for Administration Servers

This section provides the software and hardware requirements for devices used as Administration Servers. Also provided are recommendations for calculating the number and hierarchy of Administration Servers depending on the configuration of the organization's network.

## Calculation of hardware resources for the Administration Server

This section contains calculations that provide guidance for planning hardware resources for the Administration Server.

## Hardware requirements for the DBMS and the Administration Server

The following tables give the recommended minimum hardware requirements to a DBMS and Administration Server obtained during tests. For a complete list of operating systems and DBMSs supported, please refer to the list of [hardware and software requirements](#).

Administration Server, DBMS, and Web Console each on a separate device, the network includes 50 000 devices

Configuration of the device that has Administration Server installed

| Hardware        | Value                       |
|-----------------|-----------------------------|
| CPU             | 8 cores, 2500 MHz           |
| RAM             | 16 GB                       |
| Hard drive      | 300 GB, RAID 10 recommended |
| Network adapter | 1 Gbit                      |

Configuration of the device that has DBMS installed

| Hardware        | Value                       |
|-----------------|-----------------------------|
| CPU             | 16 cores, 2500 MHz          |
| RAM             | 32 GB                       |
| Hard drive      | 300 GB, RAID 10 recommended |
| Network adapter | 1 Gbit                      |

Configuration of the device that has Web Console installed

| Hardware        | Value             |
|-----------------|-------------------|
| CPU             | 4 cores, 2500 MHz |
| RAM             | 8 GB              |
| Hard drive      | 40 GB             |
| Network adapter | 1 Gbit            |

Administration Server and Web Console on the same device, DBMS on a separate device, the network includes 50 000 devices

Configuration of the device that has Administration Server and Web Console installed

| Hardware        | Value                       |
|-----------------|-----------------------------|
| CPU             | 12 cores, 2500 MHz          |
| RAM             | 24 GB                       |
| Hard drive      | 340 GB, RAID 10 recommended |
| Network adapter | 1 Gbit                      |

Configuration of the device that has DBMS installed

| Hardware        | Value                       |
|-----------------|-----------------------------|
| CPU             | 16 cores, 2500 MHz          |
| RAM             | 32 GB                       |
| Hard drive      | 300 GB, RAID 10 recommended |
| Network adapter | 1 Gbit                      |

The tests were run under the following settings:

- Automatic assignment of distribution points is enabled on the Administration Server, or distribution points are [assigned manually in accordance with the recommended table](#).
- The backup task saves backup copies to a file resource located on a dedicated server.

## Calculation of database space

The approximate amount of space that must be reserved in the database can be calculated using the following formula:

$$(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), \text{ KB}$$

where:

- C is the number of devices.
- E is the number of events to store.
- A is the total number of Active Directory objects:
  - Device accounts
  - User accounts
  - Accounts of security groups
  - Active Directory organizational units

If scanning of Active Directory is disabled, A is considered to equal zero.

- N is the average number of inventoried executable files on an endpoint device.
- F is the number of endpoint devices, where executable files were inventoried.

If you plan to enable (in the Kaspersky Endpoint Security policy settings) notification of Administration Server on applications that you run, you will need additional  $(0.03 * C)$  gigabytes to store in the database the information about applications that you run.

During operation, a certain *unallocated space* is always present in the database. Therefore, the actual size of the database file (by default, the KAV.MDF file, if you use SQL Server as the DBMS) often turns out to be approximately twice as large as the amount of space occupied in the database.

It is not recommended to limit explicitly the size of the transaction log (by default, the file KAV\_log.LDF, if you use SQL Server as the DBMS). It is recommended to leave the default value of the MAXSIZE parameter. However, if you have to limit the size of this file, take into consideration that the typical necessary value of the MAXSIZE parameter for KAV\_log.LDF is 20480 MB.

## Calculation of disk space

The Administration Server disk space required for the `/var/opt/kaspersky/klagent_srv/` folder can be estimated approximately using the formula:

$$(724 * C + 0.15 * E + 0.17 * A), \text{ KB}$$

where:

- C is the number of devices.
- E is the number of events to store.
- A is the total number of Active Directory objects:
  - Device accounts
  - User accounts
  - Accounts of security groups
  - Active Directory organizational units

If scanning of Active Directory is disabled, A is considered to equal zero.

## Calculation of the number and configuration of Administration Servers

To reduce the load on the primary Administration Server, you can assign a separate Administration Server to each administration group. The number of secondary Administration Servers cannot exceed 500 for a single primary Administration Server.

We recommend that you create the configuration of Administration Servers in correspondence to the [configuration of your organization's network](#).

## Recommendations for connecting dynamic virtual machines to Kaspersky Security Center



Dynamic virtual machines (also referred to as dynamic VMs) consume more resources than static virtual machines.

For more information on dynamic virtual machines, see [Support of dynamic virtual machines](#).

When a new dynamic VM is connected, Kaspersky Security Center Linux creates a record for this dynamic VM in Kaspersky Security Center Web Console and moves the dynamic VM to the administration group. After that, the dynamic VM is added to the Administration Server database. The Administration Server is fully synchronized with Network Agent installed on this dynamic VM.

In an organization's network, Network Agent creates the following network lists for each dynamic VM:

- Hardware
- Installed software
- Detected vulnerabilities
- Events and lists of executable files of the Application control component

The Network Agent transfers these network lists to the Administration Server. The size of the network lists depends on components installed on the dynamic VM, and may affect the performance of Kaspersky Security Center Linux and database management system (DBMS). Note that the load can grow non-linearly.

After the user finishes working with the dynamic VM and turns it off, this machine is then removed from the virtual infrastructure and entries about this machine are removed from the Administration Server database.

All these actions consume a lot of Kaspersky Security Center Linux and Administration Server database resources, and can reduce the performance of Kaspersky Security Center Linux and DBMS. We recommend that you connect up to 20,000 dynamic VMs to Kaspersky Security Center Linux.

You can connect more than 20,000 dynamic VMs to Kaspersky Security Center Linux if the connected dynamic VMs perform standard operations (for example, database updates) and consume no more than 80 percent of memory and 75–80 percent of available cores.

Changing policy settings, software or operating system on the dynamic VM can reduce or increase resource consumption. The consumption of 80–95 percent of resources is considered optimal.

## Calculations for distribution points and connection gateways

This section provides the hardware requirements for devices used as distribution points together with recommendations for calculating the number of distribution points and connection gateways depending on the configuration of the corporate network.

## Requirements for a distribution point

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.

If any remote installation tasks are pending on the Administration Server, the device with the distribution point will also require an amount of free disk space that is equal to the total size of the installation packages to be installed.

If one or multiple instances of the task for update (patch) installation and vulnerability fix are pending on the Administration Server, the device with the distribution point will also require additional free disk space, equal to twice the total size of all patches to be installed.

If you use the [scheme where distribution points receive database updates and application software modules directly from Kaspersky update servers](#), the distribution points must be connected to the internet.

## Calculating the number and configuration of distribution points

The more client devices a network contains, the more distribution points it requires. We recommend that you not disable automatic assignment of distribution points. When automatic assignment of distribution points is enabled, Administration Server assigns distribution points if the number of client devices is quite large and defines their configuration.

### Using exclusively assigned distribution points

If you plan to use certain specific devices as distribution points (that is, exclusively assigned servers), you can opt out of using automatic assignment of distribution points. In this case, make sure that the devices that you intend to make distribution points have sufficient volume of [free disk space](#), are not shut down regularly, and have Sleep mode disabled.

Number of exclusively assigned distribution points on a network that contains a single network segment, based on the number of networked devices

| Number of client devices in the 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 exclusively assigned 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)                                                                   |
| 10–100                                       | 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 in the network segment | Number of distribution points                                                                            |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Less than 300                                   | 0 (Do not assign distribution points)                                                                    |
| More than 300                                   | $(N/300 + 1)$ , where N is the number of networked devices; there must be at least 3 distribution points |

Number of workstations functioning as distribution points on a network that contains multiple network segments, based on the number of networked devices

| Number of client devices per network segment | Number of distribution points                                                                            |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Less than 10                                 | 0 (Do not assign distribution points)                                                                    |
| 10–30                                        | 1                                                                                                        |
| 31–300                                       | 2                                                                                                        |
| More than 300                                | $(N/300 + 1)$ , where N is the number of networked devices; there must be at least 3 distribution points |

If a distribution point is shut down (or not available for some other reason), the managed devices in its scope can access the Administration Server for updates.

## Calculation of the number of connection gateways

If you plan to use a connection gateway, we recommend that you designate a special device for this function.

A connection gateway can cover a maximum 10,000 managed devices.

## Logging of information about events for tasks and policies

This section provides calculations associated with event storage in the database of the Administration Server and offers recommendations on how to minimize the number of events, thereby reducing the load on the Administration Server.

By default, the properties of each task and policy provide for storing all events related to task execution and policy enforcement.

However, if a task is run quite frequently (for example, more than once per week) and on a fairly large number of devices (for example, more than 10,000), the number of events may turn out to be too large and the events may flood the database. In this case, it is recommended to select one of two options in the task settings:

- **Save events related to task progress.** In this case, the database receives only information about task launch, progress, and completion (successful, with a warning or error) from each device on which the task is run.
- **Save only task execution results.** In this case, the database receives only information about task completion (successful, with a warning or error) from each device on which the task is run.

If a policy has been defined for a fairly large number of devices (for example, more than 10,000), the number of events may also turn out to be large and the events may flood the database. In this case, it is recommended to choose only the most critical events in the policy settings and enable their logging. You are advised to disable the logging of all other events.

In doing so, you will reduce the number of events in the database, increase the speed of execution of scenarios associated with analysis of the event table in the database, and lower the risk that critical events will be overwritten by a large number of events.

You can also reduce the storage term for events associated with a task or a policy. The default period is 7 days for task-related events and 30 days for policy-related events. When changing the event storage term, consider the work procedures in place at your organization and the amount of time that the system administrator can devote to analyzing each event.

It is advisable to modify the event storage settings in any of the following cases:

- Events about changes in the intermediate states of group tasks and events about applying policies occupy a large share of all events in the Kaspersky Security Center Linux database.
- The operating system log begins showing entries about automatic removal of events when the established limit on the total number of events stored in the database is exceeded.

Choose event logging options based on the assumption that the optimal number of events coming from a single device per day must not exceed 20. You can increase this limit slightly, if necessary, but only if the number of devices on your network is relatively small (fewer than 10,000).

## Specific considerations and optimal settings of certain tasks

Certain tasks are subject to specific considerations related to the number of networked devices. This section offers recommendations on the optimal configuration of settings for such tasks.

Device discovery, the data backup task, database maintenance task, and group tasks for updating Kaspersky Endpoint Security are part of the basic functionality of Kaspersky Security Center Linux.

The inventory task is part of the Vulnerability and patch management feature and is unavailable if this feature is not activated.

## Device discovery frequency

It is not advisable to increase the default frequency of device discovery because this can create an excessive load on domain controllers. Instead, it is recommended to schedule polling at the minimum possible frequency permitted by the needs of your organization. Recommendations for calculating the optimal schedule are provided in the table below.

Device discovery schedule

| Number of networked devices | Recommended device discovery frequency |
|-----------------------------|----------------------------------------|
| Less than 10,000            | Default frequency or less              |
| 10,000 or greater           | Once per day or less                   |

## Administration Server data backup task and database maintenance task

The Administration Server stops working when the following tasks are running:

- Backup of Administration Server data

- Database maintenance

When these tasks are running, the database cannot receive any data.

You may have to reschedule these tasks so that they are not executed at the same time as other Administration Server tasks.

## Group tasks for updating Kaspersky Endpoint Security

If the Administration Server acts as the update source, the recommended schedule option for group update tasks of Kaspersky Endpoint Security 10 and later versions is **When new updates are downloaded to the repository** with the **Use automatically randomized delay for task starts** check box selected.

If a local task for downloading updates from Kaspersky servers to the repository is created on each distribution point, periodic scheduling is recommended for the Kaspersky Endpoint Security group update task. The value of the randomization period must be one hour in this case.

## Software inventory task

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 number of executable files received by the Administration Server from a single device cannot exceed 150,000. When Kaspersky Security Center Linux reaches this limit, it cannot receive any new files.

Typically, the number of files on a common client device does not exceed 60,000. The number of executable files on a file server can be greater than and even exceed the 150,000 threshold.

## Details of network load spread among Administration Server and protected devices

This section provides the results of test measurements of network traffic with a description of the conditions under which the measurements were performed. You can refer to this information when planning the network infrastructure and the throughput capacity of network channels within your organization (or between the Administration Server and another organization with devices to protect). Knowing the throughput capacity of the network, you can also estimate approximately how much time different data transmission operations will take.

## Traffic consumption under various scenarios

The table below shows the results of measuring tests conducted on traffic between the Administration Server and a managed device in different scenarios.

By default, devices are synchronized with the Administration Server [every 15 minutes or at a longer interval](#). However, if you modify the settings of a policy or a task on the Administration Server, early synchronization occurs on devices to which the policy (or task) is applicable so the new settings are transmitted to the devices.

| Scenario                                                                                                                                          | Traffic from the Administration Server to each managed device | Traffic from each managed device to the Administration Server |
|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|
| Installing Kaspersky Endpoint Security for Linux with updated databases                                                                           | 390 MB                                                        | 3.3 MB                                                        |
| Network Agent installation                                                                                                                        | 75 MB                                                         | 397 KB                                                        |
| Concurrent installation of Network Agent and Kaspersky Endpoint Security for Linux                                                                | 459 MB                                                        | 3.6 MB                                                        |
| Initial update of anti-virus databases without updating the databases in the package (if participation in Kaspersky Security Network is disabled) | 113 MB                                                        | 1.8 MB                                                        |
| Daily update of anti-virus databases (if participation in Kaspersky Security Network is enabled)                                                  | 22 MB                                                         | 373 MB                                                        |
| Initial synchronization before update of databases on a device (transfer of policies and tasks)                                                   | 382 KB                                                        | 446 KB                                                        |
| Initial synchronization after updating databases on a device                                                                                      | 20 KB                                                         | 157 KB                                                        |
| Synchronization with no changes on the Administration Server (according to schedule)                                                              | 18 KB                                                         | 23 KB                                                         |
| Synchronization when a single setting in a group policy is changed (as soon as the setting is altered)                                            | 19 KB                                                         | 20 KB                                                         |
| Synchronization when a single setting in a group task is changed (as soon as the setting is altered)                                              | 14 KB                                                         | 11 KB                                                         |
| Forced synchronization                                                                                                                            | 110 KB                                                        | 109 KB                                                        |
| <b>Virus detected</b> event (1 virus)                                                                                                             | 44 KB                                                         | 50 KB                                                         |
| <b>Virus detected</b> event (10 viruses)                                                                                                          | 58 KB                                                         | 77 KB                                                         |
| One-time traffic after enabling the Application Registry list                                                                                     | up to 10 KB                                                   | up to 12 KB                                                   |
| Everyday traffic when the Application Registry list is enabled                                                                                    | up to 840 KB                                                  | up to 1 MB                                                    |

## Average traffic usage per 24 hours

The average 24-hour traffic usage between the Administration Server and a managed device is as follows:

- Traffic from the Administration Server to the managed device is 840 KB.
- Traffic from the managed device to the Administration Server is 1 MB.

The traffic was measured under the following conditions:

- The managed device had Network Agent and Kaspersky Endpoint Security for Linux installed.
- The device was not assigned a distribution point.

- Vulnerability and patch management was not enabled.
- The frequency of synchronization with the Administration Server was 15 minutes.

# 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 can't find a solution to your issue in the Kaspersky Security Center Linux documentation or in any of the sources of information about Kaspersky Security Center Linux, contact Kaspersky Technical Support. Technical Support specialists will answer all your questions about installing and using Kaspersky Security Center Linux.

Kaspersky provides support of Kaspersky Security Center Linux during its lifecycle (see the [product 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 sending a request to 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 and store a history of them as well.

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](#) <sup>24</sup>.

## Sources of information about the application

### Kaspersky Security Center Linux page on the Kaspersky website

On the [Kaspersky Security Center Linux page on the Kaspersky website](#), you can view general information about the application, its functions, and features.

### Kaspersky Security Center Linux page in the Knowledge Base

The *Knowledge Base* is a section on the Kaspersky Technical Support website.

On the [Kaspersky Security Center Linux page in the Knowledge Base](#), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to buy, install, and use the application.

Articles in the Knowledge Base may provide answers to questions that relate both to Kaspersky Security Center Linux as well as to other Kaspersky applications. Articles in the Knowledge Base may also contain Technical Support news.

### Discuss Kaspersky applications with the community

If your question does not require an immediate answer, you can discuss it with Kaspersky experts and other users on [our Forum](#).

On the Forum, you can view discussion topics, post your comments, and create new discussion topics.

An internet connection is required to access website resources.

If you cannot find a solution to your problem, [contact Technical Support](#).

## Known issues

Kaspersky Security Center Linux has a number of limitations that are not critical to operation of the application:

- 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 your network includes a Microsoft Active Directory domain that contains several tens of thousands of objects (managed devices, security groups, and user accounts) and the response page size (the `MaxPageSize` parameter) is less than 5,000, the domain controller polling is not available and information about domain objects is not received. When you try to poll the domain controller, the *Size limit exceeded* error occurs. Increasing the response page size may help to fix the error. You can [use the Ntldsutil.exe utility](#) to increase the `MaxPageSize` parameter value to 5000 or to 10000, if necessary.
- When you enable KPSN in the Administration Server properties and use HTTPS port 17111, the connection with `ds.kaspersky.com` is not interrupted.
- Kaspersky Endpoint Security for Windows does not support the KSN Proxy service if the **Use HTTPS** option is enabled in the KSN Proxy settings of the Administration Server properties, and the Administration Server address contains non-Latin characters.
- When you switch to a secondary Server from the interface of a primary Kaspersky Security Center Linux Administration Server, the **Seamless updates** section of the main menu cannot be opened.
- When you create the *Add key* task for Kaspersky Endpoint Security 11.3 for Mac, the wizard displays a license key table that may contain empty lines.
- The protection level displayed in the Kaspersky Endpoint Security for Windows policy does not correspond to the protection level in the interface of Kaspersky Endpoint Security for Windows.
- When you run the *Uninstall application remotely* task to remove a Kaspersky application from a managed device, the task completes successfully, but the application is not removed. This issue is valid for Kaspersky Endpoint Security for Linux, Kaspersky Embedded Systems Security for Linux, and Kaspersky Industrial CyberSecurity for Linux Nodes.
- The Administration Server properties window contains settings for mobile devices, though Kaspersky Security Center Linux does not support management of mobile devices.
- If an application from the **Applications registry** section was detected on a Linux device, the application properties do not contain information about related executable files.
- If you install Network Agent on a device running the ALT Linux operating system through a remote installation task and you run this task under an account with non-root privileges, the task fails. Run the remote installation task under the root account, or create and use a stand-alone installation package of Network Agent to install the application locally.
- In reports with a letter format, a page break may cut a text line horizontally.
- In the **Add secondary Administration Server** wizard, if you specify an account with enabled two-step verification for authentication on the future secondary Server, the wizard finishes with an error. To resolve this issue, specify an account for which two-step verification is disabled or create the hierarchy from the future secondary Server.
- If you open Kaspersky Security Center Web Console in different browsers and download the Administration Server certificate file in the Administration Server properties window, the downloaded files have different

names.

- A managed device that has more than one network adapter sends Administration Server information about the MAC address of the network adapter that is not the one that is used to connect to Administration Server.
- In Astra Linux 64-bit edition, the klnagent-astra package cannot be upgraded with klnagent64\_14 package: the old package klnagent64-astra will be removed, and the new package klnagent64 will be installed instead of upgrade, so the new icon for device with klnagent64\_14 package will be added. You can remove the old icon for this device.

# Glossary

## Active key

A key that is currently used by the application.

## Additional subscription key

A key that certifies the right to use the application but is not currently being used.

## Administration Console

A component of Windows-based Kaspersky Security Center (also called MMC-based Administration Console). This component provides a user interface for the administrative services of Administration Server and Network Agent. The Administration Console is an analog of Kaspersky Security Center Web Console.

## 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 Linux that centrally stores information about all Kaspersky applications that are installed on the corporate network. It can also be used to manage these applications.

## Administration Server certificate

The certificate that the Administration Server uses for the following purposes:

- Authentication of Administration Server when connecting to Kaspersky Security Center Web Console
- Secure interaction between Administration Server and Network Agents on managed devices
- Authentication of Administration Servers when connecting a primary Administration Server to a secondary Administration Server

The certificate is created automatically when you install the Administration Server, and then stored on the Administration Server.

## Administration Server client (Client device)

A device, server, or workstation on which Network Agent is installed and managed Kaspersky applications are running.

## Administration Server data backup

Copying of the Administration Server data for backup and subsequent restoration performed by using the backup utility. The utility can save:

- Database of the Administration Server (policies, tasks, application settings, events saved on the Administration Server)
- Configuration information about the structure of administration groups and client devices
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates)
- Administration Server certificate

## Administrator rights

The level of the user's rights and privileges required for administration of Exchange objects within an Exchange organization.

## Administrator's workstation

A device from what you open Kaspersky Security Center Web Console. This component provides a Kaspersky Security Center Linux management interface.

The administrator's workstation is used to configure and manage the server side of Kaspersky Security Center Linux. Using the administrator's workstation, the administrator builds and manages a centralized anti-virus protection system for a corporate LAN based on Kaspersky applications.

## Anti-virus databases

Databases that contain information about computer security threats known to Kaspersky as of when the anti-virus databases are released. Entries in anti-virus databases allow malicious code to be detected in scanned objects. Anti-virus databases are created by Kaspersky specialists and updated hourly.

## Anti-virus protection service provider

An organization that provides a client organization with anti-virus protection services based on Kaspersky solutions.

## Application Shop

Component of Kaspersky Security Center Linux. Application Shop is used for installing applications on Android devices owned by users. Application Shop allows you to publish the APK files of applications and links to applications in Google Play.

## Authentication Agent

Interface that lets you complete authentication to access encrypted hard drives and load the operating system after the bootable hard drive has been encrypted.

## Available update

A set of updates for Kaspersky application modules, including critical updates accumulated over a certain period of time and changes to the application's architecture.

## Backup folder

Special folder for storage of Administration Server data copies created using the backup utility.

## Broadcast domain

A logical area of a network in which all nodes can exchange data using a broadcasting channel at the level of OSI (Open Systems Interconnection Basic Reference Model).

## Centralized application management

Remote application management using the administration services provided in Kaspersky Security Center.

## Client administrator

A staff member of a client organization who is responsible for monitoring the anti-virus protection status.

## Configuration profile

Policy that contains a collection of settings and restrictions for an iOS MDM mobile device.

## Connection gateway

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

## Demilitarized zone (DMZ)

Demilitarized zone is a segment of a local network that contains servers, which respond to requests from the global Web. In order to ensure the security of an organization's local network, access to the LAN from the demilitarized zone is protected with a firewall.

## Device owner

Device owner is a user whom the administrator can contact when the need arises to perform certain operations on a device.

## Direct application management

Application management through a local interface.

## 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. Distribution point was previously known as update agent.

## Event repository

A part of the Administration Server database dedicated to storage of information about events that occur in Kaspersky Security Center Linux.

## Event severity

Property of an event encountered during the operation of a Kaspersky application. There are the following severity levels:

- Critical event



- Functional failure
- Warning
- Info

Events of the same type can have different severity levels depending on the situation in which the event occurred.

## 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.

## Incompatible application

An anti-virus application from a third-party developer or a Kaspersky application that does not support management through Kaspersky Security Center Linux.

## Installation package

A set of files created for remote installation of a Kaspersky application by using the Kaspersky Security Center remote administration system. The installation package contains a range of settings needed to install the application and get it running immediately after installation. Settings correspond to application defaults. The installation package is created using files with the .kpd and .kud extensions included in the application distribution kit.

## Internal users

The accounts of internal users are used to work with virtual Administration Servers. Kaspersky Security Center Linux grants the rights of real users to internal users of the application.

The accounts of internal users are created and used only within Kaspersky Security Center Linux. No data on internal users is transferred to the operating system. Kaspersky Security Center Linux authenticates internal users.

## 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 Private Security Network (KPSN)

Kaspersky Private Security Network is a solution that gives users of devices with Kaspersky applications installed access to reputation databases of Kaspersky Security Network and other statistical data—without sending data from their devices to Kaspersky Security Network. Kaspersky Private Security Network is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:

- Devices are not connected to the internet.
- Transmission of any data outside the country or the corporate LAN is prohibited by law or corporate security policies.

## Kaspersky Security Center Linux Administrator

The person managing application operations through the Kaspersky Security Center Linux remote centralized administration system.

## Kaspersky Security Center Linux Web Server

A component of Kaspersky Security Center Linux that is installed together with Administration Server. Web Server is designed for transmission, over a network, of stand-alone installation packages, iOS MDM profiles, and files from a shared folder.

## Kaspersky Security Center Operator

A user who monitors the status and operation of a protection system managed with Kaspersky Security Center.

## Kaspersky Security Center System Health Validator (SHV)

A component of Kaspersky Security Center Linux designed for checking the operating system's operability in case of concurrent operation of Kaspersky Security Center Linux and Microsoft NAP.

## Kaspersky update servers

HTTP(S) 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.

## License term

A time period during which you have access to the application features and rights to use additional services. The services you can use depend on the type of the license.

## Licensed applications group

A group of applications created on the basis of criteria set by the administrator (for example, by vendor), for which statistics of installations on client devices are maintained.

## Local installation

Installation of a security application on a device on a corporate network that presumes manual installation startup from the distribution package of the security application or manual startup of a published installation package that was pre-downloaded to the device.

## Local task

A task defined and running on a single client computer.

## Managed devices

Corporate networked devices that are included in an administration group.

## Manual installation

Installation of a security application on a device in the corporate network from the distribution package. Manual installation requires the involvement of an administrator or another IT specialist. Usually manual installation is done if remote installation has completed with an error.

## Network Agent

A Kaspersky Security Center Linux component that enables interaction between the Administration Server and Kaspersky applications that are installed on a specific network node (workstation or server). This component is common to all of the company's applications for Microsoft® Windows®. Separate versions of Network Agent exist for Kaspersky applications developed for Unix-like OS and macOS.

## Network anti-virus protection

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. Network security increases when you use security applications and services and when you apply and adhere to the corporate data security policy.

## Network protection status

Current protection status, which defines the safety of corporate networked devices. The network protection status includes such factors as installed security applications, usage of license keys, and number and types of threats detected.

## 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 multiple policies for applications installed on computers in each administration group, but only one policy can be applied at a time to each application within an administration group.

## Profile

Collection of settings of [Exchange mobile devices](#) that define their behavior when connected to a Microsoft Exchange Server.

## Program 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.

## Protection status

Current protection status, which reflects the level of computer security.

## Provisioning profile

Collection of settings for applications' operation on iOS mobile devices. A provisioning profile contains information about the license; it is linked to a specific application.

## Remote installation

Installation of Kaspersky applications by using the services provided by Kaspersky Security Center Linux.

## Restoration

Relocation of the original object from Quarantine or Backup to its original folder where the object had been stored before it was quarantined, disinfected or deleted, or to a user-defined folder.

## Restoration of Administration Server data

Restoration of Administration Server data from the information saved in Backup by using the backup utility. The utility can restore:

- Database of the Administration Server (policies, tasks, application settings, events saved on the Administration Server)
- Configuration information about the structure of administration groups and client computers
- Repository of the installation files for remote installation of applications (content of the folders: Packages, Uninstall Updates)
- Administration Server certificate

## Role group

A group of users of Exchange ActiveSync mobile devices who have been granted identical [administrator rights](#).

## Service provider's administrator

A staff member at an anti-virus protection service provider. This administrator performs installation and maintenance jobs for anti-virus protection systems based on Kaspersky anti-virus products and also provides technical support to customers.

## Shared certificate

A certificate intended for identifying the user's mobile device.

## SSL

A data encryption protocol used on the internet and local networks. The Secure Sockets Layer (SSL) protocol is used in web applications to create a secure connection between a client and server.

## Task

Functions performed by the Kaspersky application are implemented as tasks, such as: Real-time file protection, Full computer scan, and Database update.

## Task for specific devices

A task assigned to a set of client devices from arbitrary administration groups and performed on those devices.

## Task settings

Application settings that are specific for each task type.

## Update

The procedure of replacing or adding new files (databases or application modules) retrieved from the Kaspersky update servers.

## Virtual Administration Server

A component of Kaspersky Security Center Linux, designed for management of the protection system of a client organization's network.

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

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

## Information about third-party code

Information about third-party code is contained in the file `legal_notices.txt`, in the application installation directory.

## Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Adobe, Acrobat, Flash, Shockwave and PostScript are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

AMD, AMD64 are trademarks or registered trademarks of Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace are trademarks of Amazon.com, Inc. or its affiliates.

Apache is either a registered trademark or a trademark of the Apache Software Foundation.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, and Touch ID are trademarks of Apple Inc.

Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Ubuntu, LTS are registered trademarks of Canonical Ltd.

Cisco, Cisco Systems, IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Citrix, XenServer are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Corel is a trademark or registered trademark of Corel Corporation and/or its subsidiaries in Canada, the United States and/or other countries.

Cloudflare, the Cloudflare logo, and Cloudflare Workers are trademarks and/or registered trademarks of Cloudflare, Inc. in the United States and other jurisdictions.

Dropbox is a trademark of Dropbox, Inc.

Firebird is a registered trademark of the Firebird Foundation.

Foxit is a registered trademark of Foxit Corporation.

FreeBSD is a registered trademark of The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Google Public DNS, Hangouts, and YouTube are trademarks of Google LLC.

EulerOS, FusionCompute, FusionSphere are trademarks of Huawei Technologies Co., Ltd.

Intel, Core, Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

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.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista, and Windows Azure are trademarks of the Microsoft group of companies.

Mozilla, Firefox, Thunderbird are trademarks of the Mozilla Foundation in the U.S. and other countries.

Novell is a registered trademark of Novell Enterprises Inc. in the United States and other countries.

OpenSSL is a trademark owned by the OpenSSL Software Foundation.

Oracle, Java, JavaScript, and TouchDown are registered trademarks of Oracle and/or its affiliates.

Parallels, the Parallels logo, and Coherence are trademarks or registered trademarks of Parallels International GmbH.

Chef is a trademark or registered trademark of Progress Software Corporation and/or one of its subsidiaries or affiliates in the U.S. and/or other countries.

Puppet is a trademark or registered trademark of Puppet, Inc.

Python is a trademark or registered trademark of the Python Software Foundation.

Red Hat, Fedora, and Red Hat Enterprise Linux are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Ansible is a registered trademark of Red Hat, Inc. in the United States and other countries.

CentOS is a trademark or registered trademark of Red Hat, Inc. or its subsidiaries in the United States and other countries.

BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

Debian is a registered trademark of Software in the Public Interest, Inc.

Splunk, SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries.

SUSE is a registered trademark of SUSE LLC in the United States and other countries.

Symbian trademark is owned by the Symbian Foundation Ltd.

OpenAPI is a trademark of The Linux Foundation.

VMware, VMware vSphere, VMware Workstation are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Zabbix is a registered trademark of Zabbix SIA.