Kaspersky Thin Client

Contents

Kaspersky Thin Client Help

	What's new Find out what's new in this version of Kaspersky Thin Client.		**Hardware and software requirements** Check the requirements for remote desktops and connected peripheral devices.
	Update How to update the version of Kaspersky Thin Client.		**Reset of settings and data** How to reset Kaspersky Thin Client settings and data.
	Getting started How to configure Kaspersky Thin Client settings. How to switch Kaspersky Thin Client to trusted mode. How to connect to a remote desktop.		**Advanced capabilities** Managing Kaspersky Thin Client certificates. Managing policies. Managing power-saving mode. Managing access to Kaspersky Thin Client settings.
	Monitoring events How to send event and audit logs to a log server. How to view Kaspersky Thin Client events through the Kaspersky Security Center Web Console.		**Licensing** Find out how to license Kaspersky Thin Client.

About Kaspersky Thin Client

Kaspersky Thin Client version 1.6.1 beta (hereinafter also referred to as "Kaspersky Thin Client" or "the system") is an operating system for thin clients based on the KasperskyOS operating system. Kaspersky Thin Client is designed to provide users with access to a remote desktop and serves as a substitute for a local workstation. Kaspersky Thin Client version 1.6.1 beta can be installed only to a TONK TN1200 thin client.

> Kaspersky Thin Client version 1.6.1 beta is distributed exclusively to conduct testing in the information and communication environments used in legal entities.

Core functions of Kaspersky Thin Client:

- Connect to physical and virtual desktops running Microsoft® Windows® operating systems via Remote Desktop Protocol (RDP), and by using the Microsoft Remote Desktop Connection Broker, with authorization based on a user name and password.
- Connect to terminal servers running Microsoft Windows Server® operating systems via Remote Desktop Protocol (RDP), and by using the Microsoft Remote Desktop Connection Broker, with authorization based on a user name and password.
- Connect to physical and virtual desktops running Linux® operating systems via Remote Desktop Protocol (RDP) with user name and password authorization.
- Connect to virtual desktops deployed in Basis.WorkPlace virtual workstation infrastructure with user name and password authorization.
- Transmit the remote desktop screen image to the monitor connected to Kaspersky Thin Client.
- Transmit events from the keyboard and mouse connected to Kaspersky Thin Client to the remote desktop.
- Transmit flash drives, smart cards, USB tokens, and printers connected to Kaspersky Thin Client to the remote desktop.
- Centrally control, update and monitor Kaspersky Thin Client via Kaspersky Security Center Web Console version 13.2 and 14.

Kaspersky Thin Client is part of the Kaspersky Secure Remote Workspace comprehensive solution. This solution also includes the Kaspersky Security Center Web Console designed for centralized administration and monitoring of thin clients with Kaspersky Thin Client. Management of thin clients through the Kaspersky Security Center Web Console is enabled by the Kaspersky Security Management Suite web plug-in (included in the distribution kit).

Distribution kit

The Kaspersky Thin Client distribution kit includes the following:

- Archive containing the installation image for Kaspersky Thin Client: Kaspersky_Thin_Client_<version number>.tar.gz.
- Text file containing information about third-party code: LegalNotices_en.txt.
- Text files containing a description of the new functionality and known limitations: ReleaseNotes_Kaspersky_Thin_Client_<version number>_RU.txt,

ReleaseNotes_Kaspersky_Thin_Client_<version number>_EN.txt.

- Files containing the Kaspersky Thin Client End User License Agreement: eula_ru_ktc_<version number>.txt, eula_en_ktc_<version number>.txt.

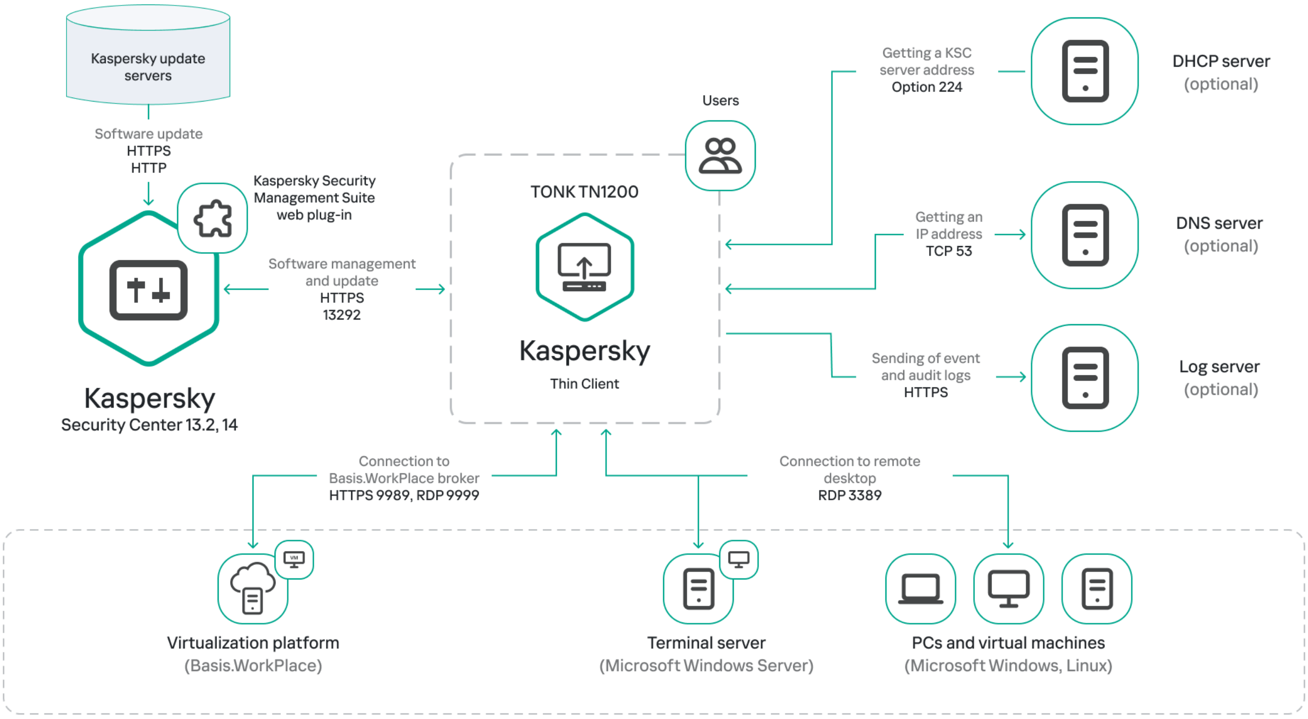
The Kaspersky Security Management Suite distribution kit includes the following:

- Archive containing the installation image and web plug-in signature file for the Kaspersky Security Center Web Console: Web_Plugin_Kaspersky_Security_Management_Suite_<plug-in version number>_ru.exe.
- Archive containing the installation image and web plug-in signature file for the Kaspersky Security Center Web Console: Web_Plugin_Kaspersky_Security_Management_Suite_<plug-in version number>_en.exe.
- Text file containing information about third-party code: KSMS_LegalNotices_en.txt.
- Text files containing a description of the new functionality and known limitations: ReleaseNotes_Kaspersky_Thin_Client_<version number>_RU.txt, ReleaseNotes_Kaspersky_Thin_Client_<version number>_EN.txt.
- Files containing the Kaspersky Security Management Suite End User License Agreement: eula_ru_ksms_<version number>.rtf, eula_en_ksms_<version number>.rtf.

Operation of Kaspersky Thin Client

The standard operating scenario for Kaspersky Thin Client (see the figure below) involves the following:

- After Kaspersky Thin Client is installed to the appropriate hardware platform, it receives network settings from a DHCP server, or the administrator manually configures these settings.
- The administrator connects and configures interaction between Kaspersky Thin Client and Kaspersky Security Center.
- Kaspersky Thin Client receives the remote desktop connection settings, updates, trusted certificates, as well as the date and time with the policy from Kaspersky Security Center.
- The user connects to the remote desktop via RDP or through the Basis.WorkPlace virtualization platform.
- In the Kaspersky Thin Client interface, the user sends audit and event logs to a recipient log server.
- Kaspersky Thin Client uses Kaspersky Security Center to receive software updates from the Kaspersky update server.



Standard operating scenario for Kaspersky Thin Client

Hardware and software requirements

This section describes the hardware and software requirements for Kaspersky Thin Client.

Requirements for monitors connected to Kaspersky Thin Client

Kaspersky Thin Client supports connection of two monitors.

Kaspersky Thin Client supports the following monitor resolutions:

- 1024x768
- 1280x800
- 1280x1024
- 1366x768
- 1440x900
- 1600x900
- 1680x1050
- 1920x1080
- 1920x1200. When connecting a monitor with this resolution, the actual resolution displayed will be no more than 1920x1080.

Kaspersky Thin Client supports the following connection interfaces:

- HDMI
- Display Port

Kaspersky Thin Client supports only True Color monitors.

Requirements for peripheral devices connected to Kaspersky Thin Client

Kaspersky Thin Client supports input from a standard USB keyboard and mouse without multimedia functionality. If necessary, you can connect and/or disconnect a keyboard and/or a mouse through the USB ports while Kaspersky Thin Client is running. You can only switch keyboard layout using the ALT+SHIFT key combination. This key combination cannot be customized. Kaspersky Thin Client supports operations with printers that are connected through USB ports. The remote computer must have the installed driver for the printer that is connected to the thin client.

Requirements for remote desktops

You can connect to physical computers, virtual machines and terminal servers that have one of the following operating systems installed:

- Microsoft Windows 7
- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Astra Linux Common Edition 2.12.43
- Astra Linux Special Edition 1.7
- ALT Linux 10
- RED OS® 7.3

Requirements for Basis.WorkPlace remote desktops

Kaspersky Thin Client supports operation with Basis.WorkPlace virtualization platform version 1.96. You can use the Basis.WorkPlace broker to connect to virtual desktops running one of the following operating systems:

- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2016

- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Astra Linux Common Edition 2.12.43
- Astra Linux Special Edition 1.7
- ALT Linux 10
- RED OS 7.3

Network requirements

The network transmission speed must be at least 50 Mbit/s.

Requirements for Kaspersky Security Center and the Kaspersky Security Center Web Console

The Kaspersky Thin Client system is compatible with Kaspersky Security Center versions 13.2 and 14. System and software requirements for the server where Kaspersky Security Center is deployed, are shown in the Kaspersky Security Center Online Help Guide ↗ .

Requirements for event logs servers

The log server that will receive the Kaspersky Thin Client audit and event logs is deployed in your enterprise infrastructure by the customer's experts.

The log server has the following requirements:

- Kaspersky Thin Client connects to the log server over HTTPS (port 443 is used by default).
- Kaspersky Thin Client connects to the log server only based on the security certificate.
- Kaspersky Thin Client receives logs by using the PUT method.

What's new

Kaspersky Thin Client version 1.6.1 beta has the following new capabilities and improvements:

- Connections via Microsoft Remote Desktop Connection Broker: added capability to connect to remote desktops running Microsoft Windows operating systems by using the Microsoft Remote Desktop Connection Broker.
- Automatic connection after unexpected disconnection: added capability to automatically connect to a remote desktop via RDP after the connection is unexpectedly disrupted.
- Expanded support for guest operating systems: added capability to connect to remote desktops running Microsoft Windows 11 or Microsoft Windows Server 2022.
- Redirection of a printer to a remote desktop: added capability to print documents from a guest operating system (when connected via RDP) on a printer that is connected to the thin client.
- Support for a new configuration of TONK TN1200: added capability ensuring that Kaspersky Thin Client can start and operate on TONK TN1200 devices with a mSATA hard drive.
- Improved performance of Kaspersky Thin Client: the speed of connection to remote desktops based on their domain name has been increased.
- Improved thin client performance: improved operational stability of a thin client connected to Kaspersky Security Center.

Installing Kaspersky Thin Client

Installation of Kaspersky Thin Client on the hardware platform is performed by TONK experts.

Kaspersky Thin Client interface

The Kaspersky Thin Client interface contains the following elements:

- Main window of the Kaspersky Thin Client. In the main window you can choose a direct connection to a remote desktop via RDP or a connection to remote desktops managed by Basis.WorkPlace. In the connection window, you can configure the RDP connection settings or the Basis.WorkPlace connection settings. If Kaspersky Thin Client is a member of an administration group and the administrator's contact details are specified in the group's general settings, the contacts of the Kaspersky Security Center administrator are also displayed in the main window.

- Control panel of Kaspersky Thin Client. It contains the following items:

  - ⏻ — shutdown button. Lets you turn off or restart Kaspersky Thin Client.

  - ⚙ — button for switching to the **Settings** and **Tools** sections:

    In the **Settings** section, you can configure Kaspersky Thin Client.

    In the **Tools** section, you can do the following:

    - View information about Kaspersky Thin Client.
    - View information about the network status.
    - View and forward Kaspersky Thin Client event logs.
    - Update Kaspersky Thin Client.
    - View the current End User License Agreement.
    - View information about third-party code.
    - Manage access to Kaspersky Thin Client settings.

  - Notification area showing the following:

    - Status of Kaspersky Thin Client connections to the network and to Kaspersky Security Center.
    - Information on new notifications of Kaspersky Thin Client.

  - Keyboard input language selection button.

  - System date and time.

After connection and during a remote desktop connection session, the upper part of the screen displays the connection panel. The connection panel displays the name of the remote desktop and the name of the connected user. When you connect to a remote desktop the connection panel is collapsed and its buttons are hidden. You can move the connection panel horizontally to the right or left by clicking the panel and waiting for an arrow to appear.

The connection panel can be expanded by using one of the following methods:

- Left-click the connection panel.
- Press the key combination `CTRL+ALT+HOME`.

The expanded connection panel displays the **Disconnect from server** button, which closes the remote desktop connection session. You can also close the connection session by pressing **`CTRL+D`**.

Kaspersky Thin Client licensing

The Kaspersky Thin Client terms of use are set forth in the End User License Agreement or a similar document regulating usage of the application.

The *End User License Agreement* is a legally binding agreement between you and AO Kaspersky Lab that stipulates the terms on which you can use Kaspersky Thin Client.

Carefully read the terms and conditions of the End User License Agreement before you start working with Kaspersky Thin Client.

You accept the terms and conditions of the End User License Agreement by confirming that you agree with the End User License Agreement text when the application starts for the first time. If you do not accept the terms and conditions of the End User License Agreement, you must cancel startup of Kaspersky Thin Client and stop using the application. When Kaspersky Thin Client is updated, any changes to the terms and conditions of the End User License Agreement for the new version of Kaspersky Thin Client are accepted by the Kaspersky Security Center administrator.

If necessary, you can view the text of the End User License Agreement in the Kaspersky Thin Client interface.

To view the text of the End User License Agreement,

In the Kaspersky Thin Client control panel, click ⬢ and select **Tools** → **End User License Agreement** in the menu that opens.

This opens a window showing the text of the End User License Agreement for the current version of Kaspersky Thin Client.

Data provision

Kaspersky Thin Client does not send any data to Kaspersky. Data is processed on the devices with Kaspersky Thin Client installed, and on the local infrastructure servers that interact with Kaspersky Thin Client.

Kaspersky Thin Client saves the following information on the device:

- Event log containing technical data on system operation and information about Kaspersky Thin Client events sent to the Kaspersky Security Center Server.
- Audit log containing data on certificates uploaded to Kaspersky Thin Client and information on instances of enabling and disabling management of thin clients via Kaspersky Security Center.
- Thin client settings:
  - Date and time when Kaspersky Thin Client was installed on the device.
  - Thin client name.
  - Currently installed version of Kaspersky Thin Client.
  - Kaspersky Thin Client interface language.
  - List of languages available when switching the keyboard input language.
  - Information about primary and secondary monitors.
  - Primary monitor ID.
  - Location (coordinates) of the connection panel.
  - Time when certificates were last used for authenticating connections: to Kaspersky Security Center, to remote desktops via RDP or via Basis.WorkPlace, and to the log server.
- Settings for working with Kaspersky Security Center:
  - Address (name or IP address and port) of Kaspersky Security Center Administration Server.
  - Kaspersky Security Center connection method (manually or via DHCP).
  - Set of Kaspersky Thin Client identifiers for connecting to Kaspersky Security Center.
  - Heartbeat interval (minutes) for synchronizing Kaspersky Thin Client with Kaspersky Security Center.
  - Number of certificates received from Kaspersky Security Center to authenticate the connections between Kaspersky Thin Client and remote desktops, the Basis.WorkPlace connection manager, and the log server.
  - Current certificate fingerprint for authenticating Kaspersky Thin Client connection to Kaspersky Security Center.
  - Kaspersky Thin Client naming settings (name, device ID, and additional information) specified by the Kaspersky Security Center administrator.
  - Set of secrets for confirming user actions in the Kaspersky Thin Client interface: resetting data and settings, disconnecting the thin client from Kaspersky Security Center, and replacing the certificate for connecting the thin client to Kaspersky Security Center.

  - Technical support contact details.
  - Certificate files for authenticating Kaspersky Thin Client connection to Kaspersky Security Center.
- Basis.WorkPlace connection settings:
  - Address (name or IP address and port) of the Basis.WorkPlace connection manager.
  - User name for connecting to the Basis.WorkPlace connection manager.
  - Certificate files for authenticating the connection broker when connecting to a remote desktop managed by Basis.WorkPlace.
  - Number of reconnection attempts.
  - Type of connection between Kaspersky Thin Client and the Basis.WorkPlace connection broker.
  - Settings for redirecting local devices to the remote desktop: whether redirection of USB devices and smart cards is enabled or disabled.
  - Whether use of two monitors is enabled or disabled.
- RDP server connection settings:
  - Address (name or IP address and port) of the RDP server.
  - Domain and user name for connecting to the RDP server.
  - Remote Desktop Connection Broker collection ID.
  - Certificate files for authenticating the RDP server when connecting to a remote desktop via RDP.
  - Settings for redirecting local devices to the remote desktop:
    - Whether USB devices redirection is enabled or disabled.
    - Whether smart cards redirection is enabled or disabled.
    - Whether redirection of printers is enabled or disabled.
  - Whether use of two monitors is enabled or disabled.
  - Whether automatic connection to the remote desktop after unexpected disconnection is enabled or disabled.
  - Image quality settings:
    - Whether font smoothing is enabled or disabled.
    - Whether menu animation is enabled or disabled.
    - Whether the desktop background is displayed.
    - Whether window contents are rendered while dragging.
    - Whether Windows themes are enabled or disabled.

- Network settings:
  - Whether automatic network configuration via DHCP is enabled or disabled.
  - Thin client IP address.
  - Subnet mask.
  - List of IP addresses of DNS servers.
  - IP address of the network gateway.
- Power-saving mode settings: the number of minutes before the monitor turns off and the number of minutes before the thin client turns off when Kaspersky Thin Client is idle.
- Log server connection settings:
  - Address (name or IP address and port) of the log server used for forwarding audit and event logs.
  - Certificate files for authenticating the log server when Kaspersky Thin Client connects to this server.
- Date and time settings:
  - Date and time received from the Administration Server during the last synchronization with Kaspersky Security Center.
  - Time zone.
- Information about available and downloaded Kaspersky Thin Client updates:
  - Update availability status.
  - Update installation status.
  - Update delivery status.
  - Available update data: Kaspersky Thin Client version, release name, date and time, importance.
  - Time of the last successful update check.
  - Time of the last successful update installation.
- Information about Kaspersky Thin Client End User License Agreements:
  - End User License Agreement IDs.
  - Texts of the End User License Agreements in English and in Russian.
  - Information about whether or not the End User License Agreements were accepted.
  - Information about the release dates of the End User License Agreements.

The Basis.WorkPlace virtualization system saves the following information in the database:

- User name.

- IP address of Kaspersky Thin Client.
- ID of Kaspersky Thin Client.
- Session startup events.
- Session termination events.

The name or IP address of the RDP server and Basis.WorkPlace connection manager are overwritten each time a connection is successfully established.

The user name is overwritten upon each successful connection to the RDP server or Basis.WorkPlace connection manager.

The log server address used for audit and event log forwarding is overwritten each time system events are successfully sent to the log server. When an audit and event log is forwarded, all system events saved on the thin client are sent to the log server.

Any received information is protected by Kaspersky in accordance with the requirements established by law and in accordance with current Kaspersky regulations. Data is transmitted over encrypted communication channels.

Turning Kaspersky Thin Client on and off

Before you start working with Kaspersky Thin Client, you must connect a mouse, keyboard and monitor to the thin client via the corresponding ports on the back panel of the device. To start working with Kaspersky Thin Client, you need to turn on the thin client. Kaspersky Thin Client lets you connect a mouse, keyboard and monitor to the thin client while the system is running.

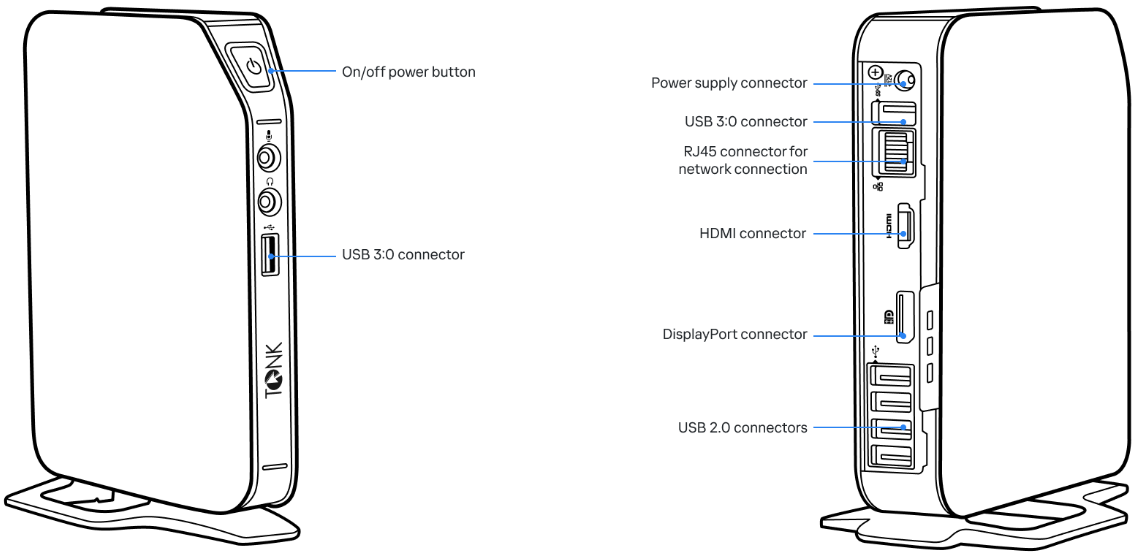
To turn on Kaspersky Thin Client,

Click the on/off power button in the upper part of the front panel of the thin client.

As a result, Kaspersky Thin Client will start running on the thin client.

While Kaspersky Thin Client is starting, the monitor connected to the thin client will sequentially display the splash screen of the thin client vendor, the welcome screen of the bootloader, the boot logs, and the dynamic splash screen when loading Kaspersky Thin Client. The appearance of the Kaspersky Thin Client main window on the screen indicates that the system is on.

> When Kaspersky Thin Client is started for the first time, the End User License Agreement acceptance window is displayed. To continue working with Kaspersky Thin Client, you need to carefully read and accept the End User License Agreement.



Front and back panels of the TONK TN1200 thin client

After you finished working with Kaspersky Thin Client, you must turn it off.

To turn off Kaspersky Thin Client:

1. In the main window of Kaspersky Thin Client, click the shutdown button on the control panel ⏻.
2. In the menu that opens, select **Shut down**.

Kaspersky Thin Client will be turned off.

Restarting Kaspersky Thin Client

You can restart Kaspersky Thin Client if necessary. For example, you may need to restart Kaspersky Thin Client to apply your selected language for the Kaspersky Thin Client interface.

To restart Kaspersky Thin Client:

1. In the main window of Kaspersky Thin Client, click the shutdown button on the control panel ⏻.
2. In the menu that opens, select **Restart**.

   Kaspersky Thin Client will be restarted.

Configuring Kaspersky Thin Client

This section describes how to configure Kaspersky Thin Client.

Scenario: Quick Start for administrators

This section describes the sequence of steps that must be performed by the administrator to install and configure Kaspersky Thin Client and Kaspersky Security Center, and to establish a connection between them.

The scenario for installing Kaspersky Thin Client and Kaspersky Security Center and configuring a connection between them consists of the following steps:

1. **Installing Kaspersky Security Center**

   Download the Kaspersky Security Center distribution package and install the full version of Kaspersky Security Center on the server. The distribution package for the full version of Kaspersky Security Center includes the Kaspersky Security Center Web Console. We recommend selecting the standard installation. For details on installing Kaspersky Security Center, please refer to the *Installation of Kaspersky Security Center* section of the Kaspersky Security Center Online Help Guide.

2. **Configuring firewall rules**

   If you plan to use the default port to connect the thin client to Kaspersky Security Center, set the rules allowing TCP connections through port 13292 for the operating system firewall of the server on which Kaspersky Security Center is installed. If you plan to use a port other than 13292, set the permissions accordingly. For detailed information on configuring firewall rules, please refer to the relevant documentation on the operating system you are using.

3. **Installing the Kaspersky Security Management Suite web plug-in**

   In the Kaspersky Security Center Web Console, install the Kaspersky Security Management Suite web plug-in. A ZIP archive containing the web plug-in distribution package is included in the distribution kit.

4. **Preparing ports**

   Kaspersky Thin Client uses a mobile protocol to connect to Kaspersky Security Center. On the Kaspersky Security Center Administration Server, enable use of the TCP port that you set up access to in step 2. For details on TCP port enabling on the Kaspersky Security Center Administration Server, see the *Modifying the Mobile Device Management settings* section of the Kaspersky Security Center Online Help Guide.

5. **Turning on Kaspersky Thin Client**

   Turn on Kaspersky Thin Client and wait for the system to load. Please read the terms and conditions of the End User License Agreement and accept the agreement.

6. **Configuring Kaspersky Thin Client settings**

   After turning on Kaspersky Thin Client and accepting the End User License Agreement, configure general settings and network connection settings.

7. **Configuring a connection between Kaspersky Thin Client and Kaspersky Security Center**

   In the Kaspersky Thin Client interface, configure the connection to Kaspersky Security Center.

8. **Adding Kaspersky Thin Client to the list of managed devices**

   Connect to the Kaspersky Security Center Web Console and add Kaspersky Thin Client to the list of managed devices in Kaspersky Security Center. Policies in the Kaspersky Security Center Web Console are applied only for managed devices.

9. **Creating an active Kaspersky Security Center policy for Kaspersky Thin Client**

   If you need to manage a group of devices, create an active policy for Kaspersky Thin Client.

10. **Enabling trusted mode for a group of devices**

    Switch devices in an administration group to trusted mode. We also recommend adding a reserve certificate for connecting Kaspersky Thin Client to Kaspersky Security Center.

When these actions are complete, Kaspersky Thin Client will be ready for operation. You will be able to manage Kaspersky Thin Client through the Kaspersky Thin Client interface or through the Kaspersky Security Center Web Console, and monitor events of Kaspersky Thin Client.

Scenario: Migrating management of Kaspersky Thin Client to a new Kaspersky Security Center Server

This section describes the sequence of steps that must be performed by the administrator when connecting a group of devices running Kaspersky Thin Client to a new Kaspersky Security Center Administration Server if this group was previously managed by a different instance of Kaspersky Security Center.

The scenario for configuring Kaspersky Thin Client management when migrating to a new instance of Kaspersky Security Center consists of the following steps:

1. **Installing a new Kaspersky Security Center Administration Server**

   Download the Kaspersky Security Center distribution package and install the full version of Kaspersky Security Center on the server. The distribution package for the full version of Kaspersky Security Center includes the Kaspersky Security Center Web Console. We recommend selecting the standard installation. For details on installing Kaspersky Security Center, please refer to the *Installation of Kaspersky Security Center* ↗ section of the Kaspersky Security Center Online Help Guide.

2. **Configuring firewall rules**

   If you plan to use the default port to connect the thin client to Kaspersky Security Center, set the rules allowing TCP connections through port 13292 for the operating system firewall of the server on which Kaspersky Security Center is installed. If you plan to use a port other than 13292, set the permissions accordingly. For detailed information on configuring firewall rules, please refer to the relevant documentation on the operating system you are using.

3. **Installing the Kaspersky Security Management Suite web plug-in**

   In the Web Console, install the Kaspersky Security Management Suite web plug-in for the new Kaspersky Security Center Administration Server. A ZIP archive containing the web plug-in distribution package is included in the distribution kit.

4. **Preparing ports**

   Kaspersky Thin Client uses a mobile protocol to connect to Kaspersky Security Center. On the Kaspersky Security Center Administration Server, enable use of the TCP port that you set up access to in step 2. For details on TCP port enabling on the Kaspersky Security Center Administration Server, see the *Modifying the Mobile Device Management settings* ↗ section of the Kaspersky Security Center Online Help Guide.

5. **Turning on Kaspersky Thin Client**

   Turn on Kaspersky Thin Client and wait for the system to load.

6. **Creating an active Kaspersky Security Center policy for Kaspersky Thin Client**

In the previously used Web Console, create an active policy for the group of devices that will be managed through the new instance of Kaspersky Security Center.

7. **Saving the mobile certificate of the new Kaspersky Security Center Administration Server**

   Locally save the mobile certificate of the new Kaspersky Security Center Administration Server.

8. **Uploading a reserve certificate in the utilized Kaspersky Security Center Web Console**

   Upload the mobile certificate of the new Kaspersky Security Center Administration Server as the reserve certificate in the previously used Kaspersky Security Center Web Console. If necessary, a user certificate for connecting Kaspersky Thin Client to Kaspersky Security Center can be uploaded as a reserve certificate. To do so, you must first create a user certificate and upload it in the Kaspersky Security Center Web Console.

   Wait for Kaspersky Thin Client to fully synchronize with Kaspersky Security Center. The synchronization period (heartbeat) is defined when configuring Kaspersky Thin Client through the Kaspersky Security Center Web Console. After synchronization, devices in the administration group will receive the mobile certificates of the new Kaspersky Security Center Administration Server.

9. **Configuring a connection between Kaspersky Thin Client and the new Kaspersky Security Center**

   If a DHCP server is deployed in your enterprise infrastructure and the settings for connecting Kaspersky Thin Client to Kaspersky Security Center are received automatically, use option 224 to define the IP address or domain name of the new Kaspersky Security Center Administration Server and wait for all devices running Kaspersky Thin Client to finish synchronizing with Kaspersky Security Center.

   Devices in the administration group will be connected to the new Kaspersky Security Center Administration Server and you will be able to manage them through the Web Console interface.

   If a DHCP server is not deployed in your enterprise infrastructure, manually configure the connection to the new Kaspersky Security Center in the Kaspersky Thin Client interface.

Scenario: Switching Kaspersky Thin Client to trusted mode

Trusted mode is an operating mode of Kaspersky Thin Client in which the thin client is connected to and managed via Kaspersky Security Center. Kaspersky Security Center must be installed and configured in advance.

The scenario for switching Kaspersky Thin Client to trusted mode consists of the following steps:

1. **Configuring a connection to Kaspersky Security Center**

   In the Kaspersky Thin Client interface, configure the connection to Kaspersky Security Center.

2. **Creating an active Kaspersky Security Center policy for Kaspersky Thin Client**

   In the Kaspersky Security Center Web Console interface, create an active policy for the group of devices for which you want to enable centralized control via Kaspersky Security Center.

3. **Adding certificates for securely connecting to remote desktops**

   In the interface of the Kaspersky Security Center Web Console, add certificates for securely connecting to remote desktops (managed by Basis.WorkPlace or via RDP) and move the toggle button in the right part of the page to the **Enforced** position. Wait for Kaspersky Thin Client to fully synchronize with Kaspersky Security Center. The synchronization period (heartbeat) is defined when configuring Kaspersky Thin Client through the Kaspersky Security Center Web Console. After synchronization, devices will receive the Kaspersky Security Center Administration Server certificates.

When these actions are complete, Kaspersky Thin Client will operate in trusted mode.

In some cases, such as when switching to a new Kaspersky Security Center Administration Server, you can switch a device running Kaspersky Thin Client out of trusted mode by deleting the security certificates and disabling management of the group via Kaspersky Security Center.

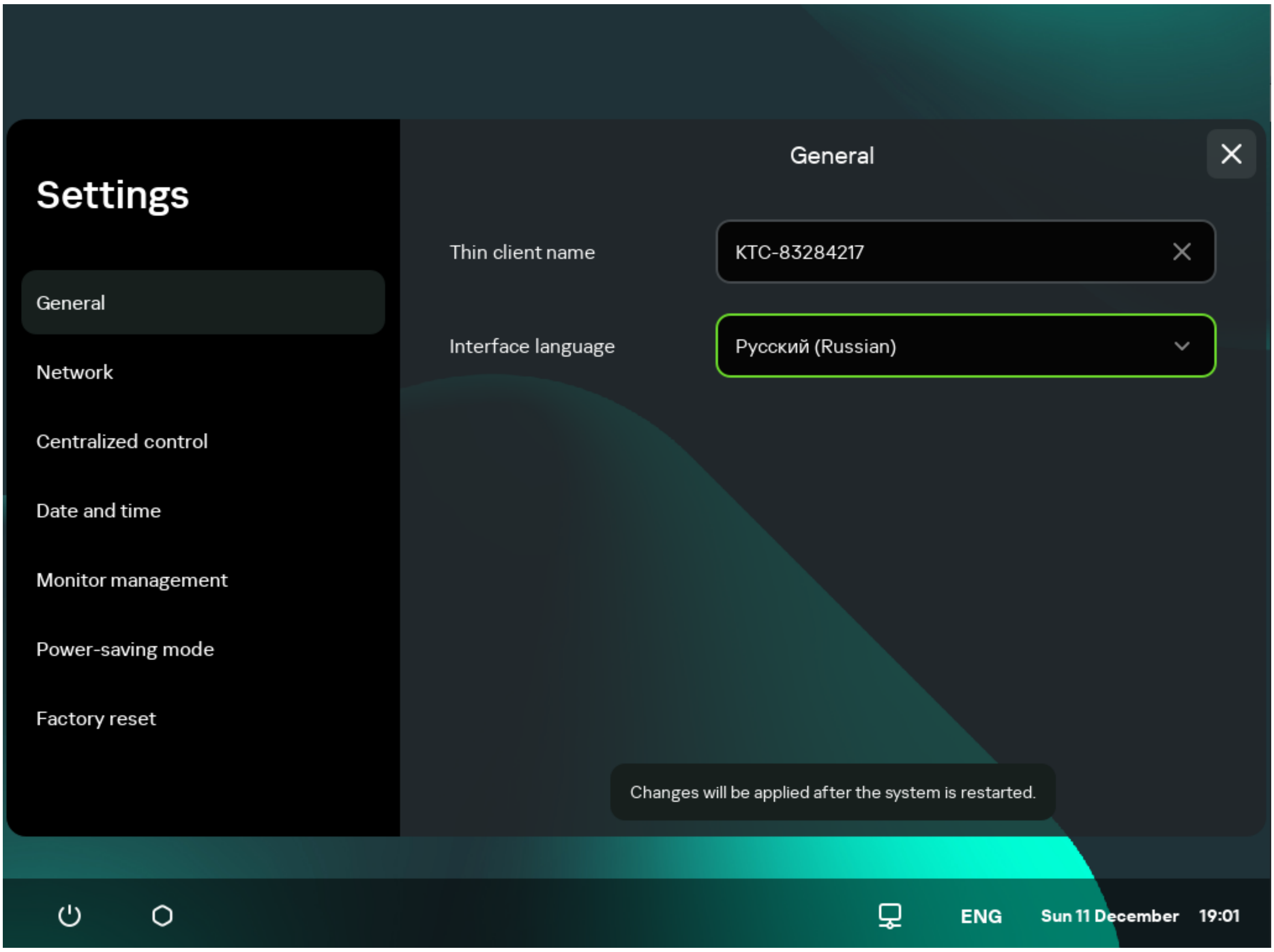
Configuring general settings

In the Kaspersky Thin Client interface, you can configure the general settings of the thin client. For example, you can specify the thin client name that will be displayed in the Kaspersky Thin Client taskbar and in the Kaspersky Security Center Web Console, and select the language of the Kaspersky Thin Client interface.

> If Kaspersky Thin Client is included in an administration group and is controlled centrally through the Web Console, the device name is assigned by the Kaspersky Security Center administrator. When the **Enforced** function is enabled, the **Thin client name** field in the Kaspersky Thin Client interface cannot be edited.

To configure general settings of Kaspersky Thin Client:

1. In the Kaspersky Thin Client control panel, click ⬡ and select **Settings** in the menu that opens.
2. In the window that opens, select the **General** section (see the figure below).



Thin client name: KTC-83284217

Interface language: Русский (Russian)

Changes will be applied after the system is restarted.

Settings. **General** section

3. In the **Thin client name** field, enter the name that will be displayed for Kaspersky Thin Client in the Web Console. The name can contain uppercase and lowercase letters of the Latin and Cyrillic alphabets, numerals and a hyphen. The length of the thin client name must not exceed 30 characters.

4. In the **Interface language** drop-down list, select the language for the Kaspersky Thin Client interface.

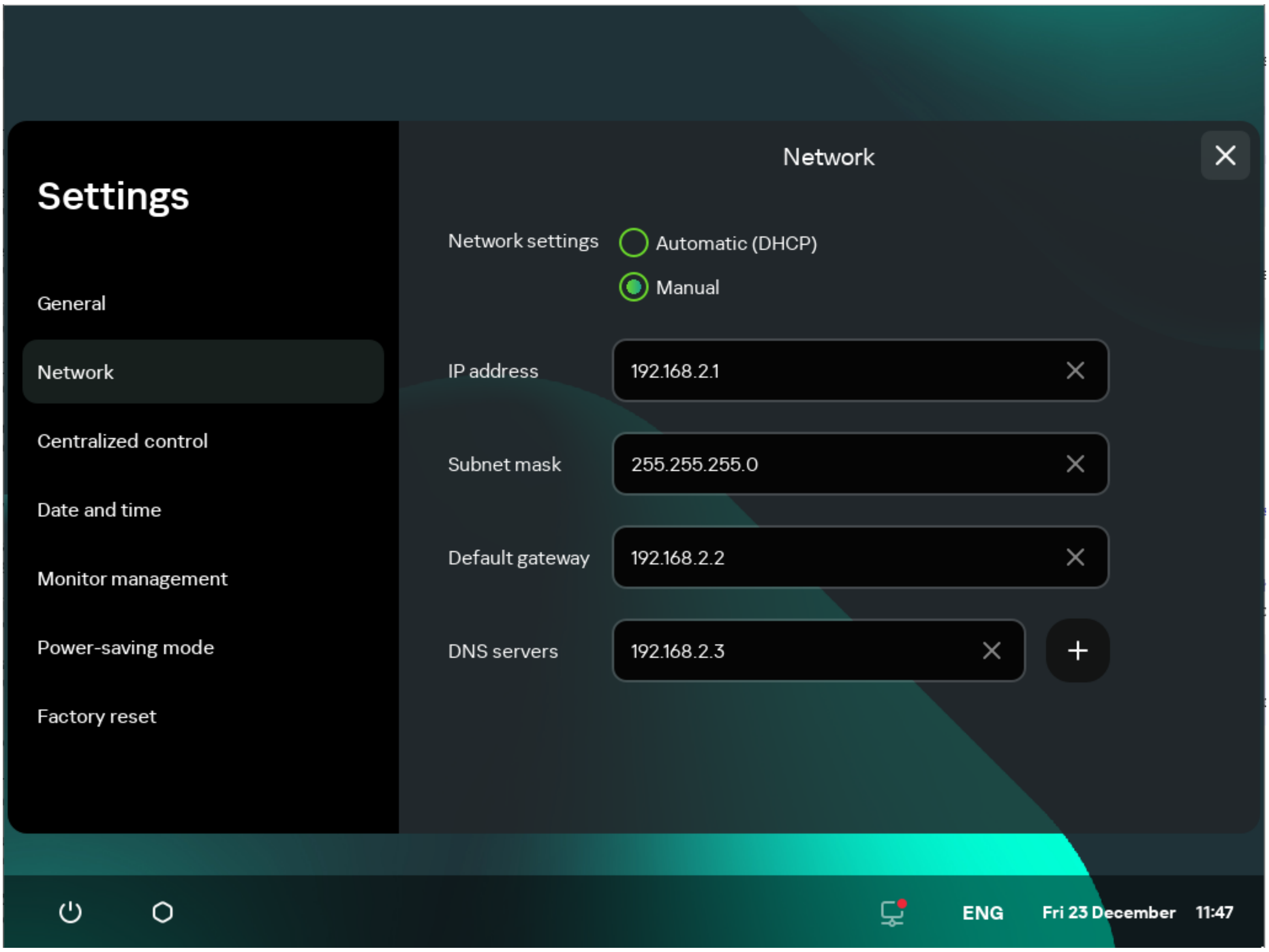
   Changes will be applied after the system is restarted.

Configuring network settings

In the **Settings** → **Network** section, you can configure the settings for connecting Kaspersky Thin Client to the network.

To configure the network settings:

1. In the Kaspersky Thin Client control panel, click ⬡ and select **Settings** in the menu that opens.
2. In the window that opens, select the **Network** section (see the figure below).



Network

Network settings ○ Automatic (DHCP) ● Manual

IP address 192.168.2.1

Subnet mask 255.255.255.0

Default gateway 192.168.2.2

DNS servers 192.168.2.3

Settings. **Network** section

3. Configure the settings for connecting Kaspersky Thin Client to the network:
   - If you need to receive the network settings automatically via DHCP, select **Automatic (DHCP)** for the **Network settings** parameter. In this mode, the **IP address**, **Subnet mask**, **Default gateway** and **DNS servers** fields are not accessible.
   - If you need to manually specify the network settings, select **Manual** for the **Network settings** parameter and do the following:
     - In the **IP address** field, enter the IP address of Kaspersky Thin Client in IPv4 format.

- In the **Subnet mask** field, enter the subnet mask.
- In the **Default gateway** field, enter the address of the network gateway.
- In the **DNS servers** field, enter the addresses of the DNS servers. You can enter no more than two addresses. This field is optional.

4. Click **Save** in the lower part of the window to save the changes.

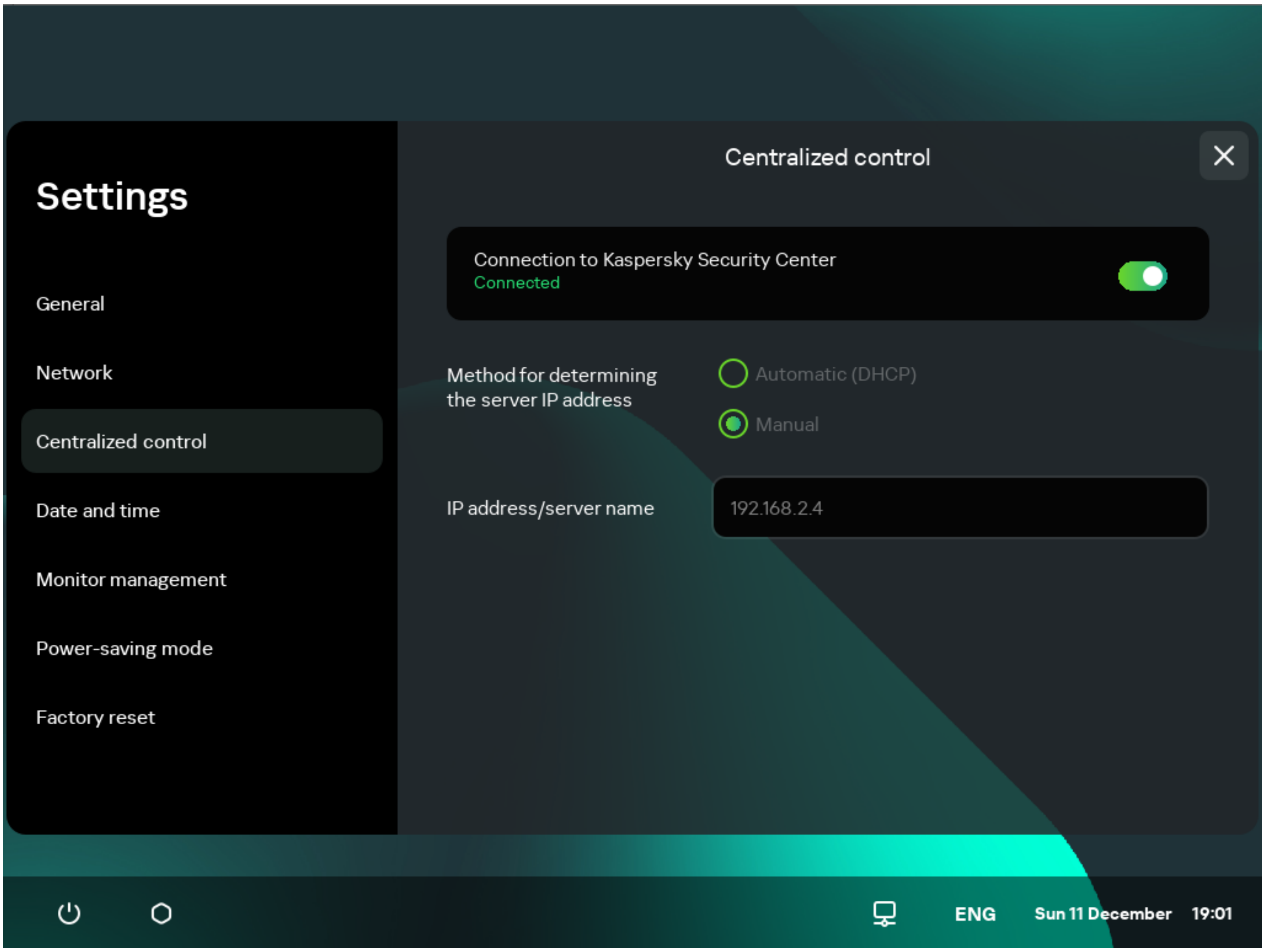
Configuring settings for connecting Kaspersky Thin Client to Kaspersky Security Center

To control a thin client through the Web Console, you must configure settings for connecting Kaspersky Thin Client to the Kaspersky Security Center Administration Server.

> If the certificate used for connecting Kaspersky Thin Client to Kaspersky Security Center has been changed in Kaspersky Security Center, you must confirm the certificate change to continue configuring the connection.

To configure settings for connecting Kaspersky Thin Client to the Kaspersky Security Center Administration Server:

1. In the Kaspersky Thin Client control panel, click ⬢ and select **Settings** in the menu that opens.
2. In the window that opens, select the **Centralized control** section (see the figure below).



Centralized control

Connection to Kaspersky Security Center
Connected

Method for determining the server IP address: ○ Automatic (DHCP) ● Manual

IP address/server name: 192.168.2.4

Settings. **Centralized control** section

3. In the **Centralized control** window that opens, configure the following settings for connecting Kaspersky Thin Client to Kaspersky Security Center:

   - If you want to use the DHCP protocol to automatically receive the settings for connecting Kaspersky Thin Client to Kaspersky Security Center, select **Automatic (DHCP)** in the **Method for determining the server IP address** block. In this mode, the **IP address/server name** field cannot be edited.

     To use this connection option, a DHCP server must be deployed in the enterprise infrastructure and option 224 must be used to define the IP address or domain name of the Kaspersky Security Center Administration Server to which you plan to connect Kaspersky Thin Client. Kaspersky Thin Client receives string values in `IP address:Port` format or `Server name:Port` format in option 224. For example, `192.168.2.4` or `ksc.example.com:12345`. The port must be specified only if a port other than port 13292 is used for the connection.

     By default, use of DHCP is enabled to automatically receive the settings for connecting Kaspersky Thin Client to Kaspersky Security Center.

   - If you want to manually define the settings for connecting Kaspersky Thin Client to Kaspersky Security Center, select **Manual** in the **Method for determining the server IP address** block and in the **IP address/server name** field enter the IP address or name of the Kaspersky Security Center Administration Server. If you are using a port other than port 13292, indicate it in `IP address:Port` format or `Server name:Port` format.

4. Activate the **Connection to Kaspersky Security Center** toggle button.

5. If you are connecting to Kaspersky Security Center for the first time, check the settings of the certificate used for connecting Kaspersky Thin Client to Kaspersky Security Center in the **Adding certificate** window and click

the **Add certificate** button. The added certificate will be used for subsequent connections between Kaspersky Thin Client and Kaspersky Security Center.

Kaspersky Thin Client will attempt to connect to Kaspersky Security Center. Following successful connection to Kaspersky Security Center, the **Connected to Kaspersky Security Center** status will be displayed.

Changing settings for connecting Kaspersky Thin Client to Kaspersky Security Center

> If Kaspersky Thin Client is a member of an administration group and is controlled centrally through the Web Console, the settings for connecting Kaspersky Thin Client to Kaspersky Security Center cannot be changed.

To change the settings for connecting Kaspersky Thin Client to Kaspersky Security Center:

1. In the Kaspersky Thin Client control panel, click ⬢ and select **Settings** in the menu that opens.
2. In the window that opens, select the **Centralized control** section.
3. Deactivate the **Connection to Kaspersky Security Center** toggle button.
4. In the **Confirm disconnection** window that opens, view and memorize the confirmation code for disconnecting Kaspersky Thin Client from Kaspersky Security Center, then provide it to the Kaspersky Security Center administrator. The administrator contact details are provided in the **Confirm disconnection** window. The administrator should send you a confirmation code in response.
5. Click **Next**.
6. In the **Confirmation code** window that opens, enter the code provided by the Kaspersky Security Center administrator and click the **Confirm** button.

   Kaspersky Thin Client will be disconnected from management through Kaspersky Security Center.
7. In the **Centralized control** window, manually configure settings for connecting to Kaspersky Security Center.
8. Activate the **Connection to Kaspersky Security Center** toggle button.

The thin client will attempt to connect to Kaspersky Security Center. Following successful connection to Kaspersky Security Center, the **Connected to Kaspersky Security Center** status will be displayed.

Managing Kaspersky Thin Client certificates

The TLS encryption protocol ensures data transfer security using SSL connection certificates. An *SSL connection certificate* (hereinafter referred to as an "SSL certificate" or simply "certificate") is a block of data containing information about the certificate owner, the owner's public key, and the start and end dates of certificate validity.

> Kaspersky Thin Client does not check to see if the certificate is on the Certificate Revocation List.

Kaspersky Thin Client uses the following certificates:

- Certificate for connecting Kaspersky Thin Client to Kaspersky Security Center.

- Certificate for authenticating the RDP server when connecting to a remote desktop.
- Certificate for authenticating the connection broker when connecting to a remote desktop managed by Basis.WorkPlace.
- Certificate for connecting to the log server.

We recommend updating certificates in the following cases:

- Current certificates have been compromised.
- Certificates have expired.
- Certificates need to be regularly updated in accordance with the information security requirements of your enterprise.

Kaspersky Thin Client uses a mobile certificate for connecting to Kaspersky Security Center. A mobile certificate is created automatically when installing Kaspersky Security Center. For details on how to reissue a mobile certificate, please refer to the *Reissuing the Web Server certificate* section of the Kaspersky Security Center Online Help Guide.

To securely connect Kaspersky Thin Client to a remote desktop via RDP, to a connection broker for remote desktops managed by Basis.WorkPlace, or to a log server, you must add the appropriate security certificate. All added certificates are saved in the system store of Kaspersky Thin Client.

For a thin client that is not in an administration group and is not managed through the Kaspersky Security Center Web Console, you can manually add a certificate in the Kaspersky Thin Client interface in the following situations:

- When connecting Kaspersky Thin Client to Kaspersky Security Center for the first time.
- When connecting to a remote desktop managed by Basis.WorkPlace or via RDP for the first time.
- When connecting to a log server for the first time.

For a thin client that is added to an administration group and is managed through the Kaspersky Security Center Web Console, the Kaspersky Security Center administrator adds certificates through the Kaspersky Security Center Web Console interface. In this case, you will be able to connect only to the servers for which the administrator added a certificate. If the certificate added to the policy is a root certificate, the connection is established based on the server domain name only.

If the Kaspersky Security Center administrator replaces the certificate for connecting to Kaspersky Security Center, some situations may require confirmation of the certificate replacement to connect to Kaspersky Security Center. For example, this may be required if the thin client was turned off for a long time, has not synchronized with Kaspersky Security Center, and the certificate previously used to connect to Kaspersky Security Center has expired.

To confirm replacement of the certificate for connecting to Kaspersky Security Center:

1. Turn on Kaspersky Thin Client.
2. In the **Certificate replacement required** window that opens, view and memorize the confirmation code and provide it to the Kaspersky Security Center administrator. The administrator contact details are provided in the **Certificate replacement required** window. The Kaspersky Security Center administrator sends you a certificate replacement code in response.
3. Click **Next**.

4. In the **Certificate replacement code** window that opens, enter the code provided by the Kaspersky Security Center administrator and click the **Confirm** button.

   As a result, the new certificate for connecting to Kaspersky Security Center will be saved in the Kaspersky Thin Client certificate store and will be subsequently used to connect to Kaspersky Security Center.

Configuring RDP connection settings

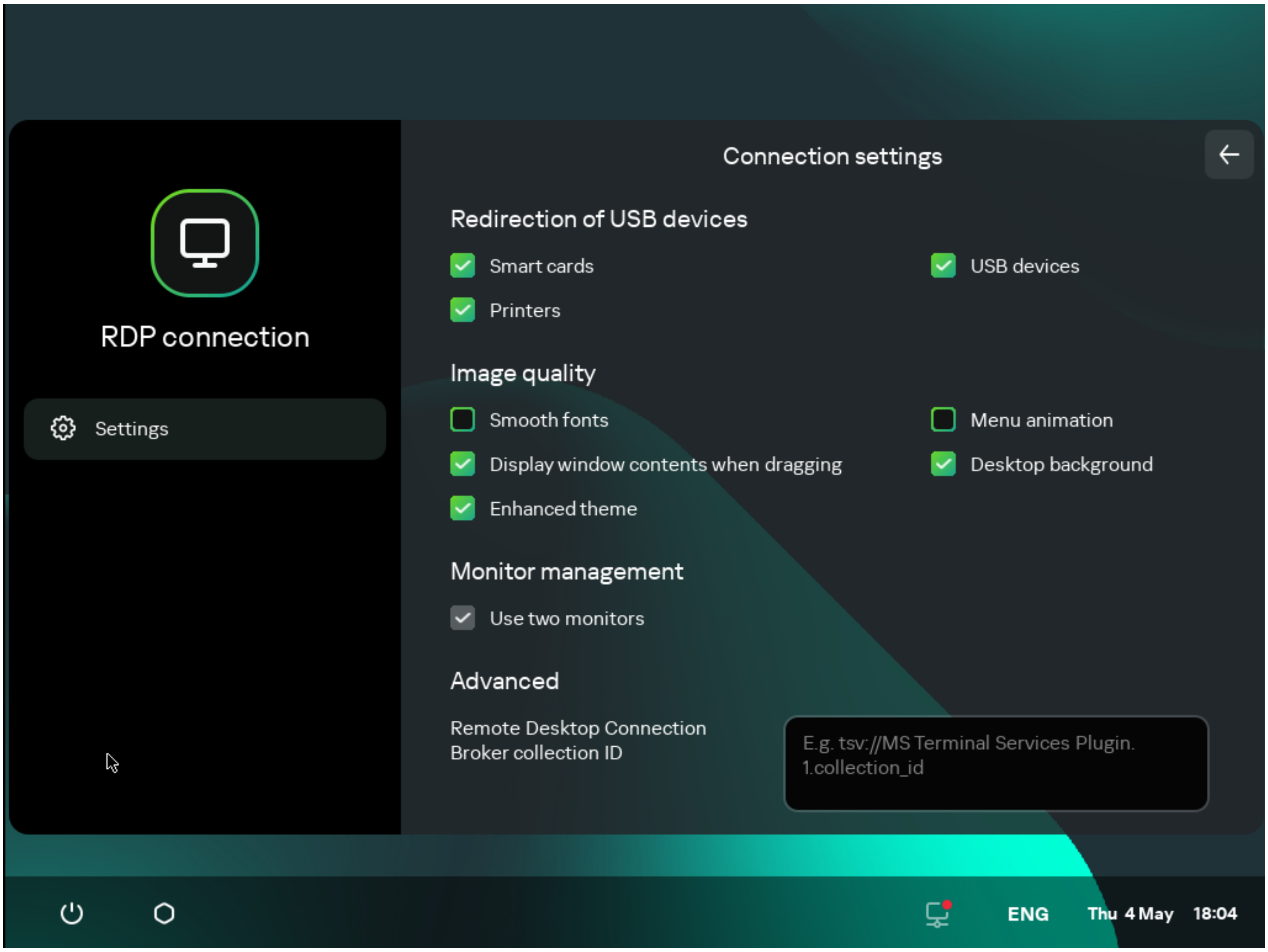
Kaspersky Thin Client lets you configure redirection of USB devices to a remote desktop, and configure settings for connecting to a remote desktop via RDP.

> To correctly redirect USB devices to a remote desktop using the Windows 10 operating system, you must enable Remote Desktop Services and allow redirection of Plug and Play devices in the settings of Remote Desktop Services. For Microsoft Windows Server 2016 and Microsoft Windows Server 2019 operating systems, you must also allow a remote connection using Remote Desktop Services and allow remote management rules to be set for user sessions in Remote Desktop Services. Redirection of smart cards, flash drives, and tokens to a remote desktop running the Microsoft Windows 7 operating system is not supported.

To configure settings for connecting to a remote desktop via RDP:

1. In the main window of Kaspersky Thin Client, click the **RDP** button.
2. In the remote desktop connection window that opens, click **Settings** in the left part of the window.

   This opens a window in which you can configure settings for connecting to a remote desktop (see the figure below).



Connection settings

Redirection of USB devices

☑ Smart cards ☑ USB devices

☑ Printers

Image quality

□ Smooth fonts □ Menu animation

☑ Display window contents when dragging ☑ Desktop background

☑ Enhanced theme

Monitor management

☑ Use two monitors

Advanced

Remote Desktop Connection Broker collection ID: E.g. tsv://MS Terminal Services Plugin.1.collection_id

3. In the **Redirection of USB devices** settings block, select the relevant check boxes next to the devices connected to the thin client via USB that you need to pass through to the remote desktop:

   - **Smart cards** if you want to enable redirection of smart cards and tokens.

   - **USB devices** if you want to enable redirection of USB devices.

   - **Printers** if you want to enable redirection of printers. The remote computer must have the installed driver for the printer that is connected to the thin client.

     All the check boxes are cleared by default.

4. In the **Image quality** block, select the check boxes next to the remote desktop graphics settings that you need to use:

   - **Smooth fonts**

   - **Menu animation**

   - **Desktop background**

   - **Display window contents when dragging**

   - **Enhanced theme**

   > Enabling remote desktop display settings may affect the speed of Kaspersky Thin Client operations.

5. If two monitors are installed at your workstation and you want a remote desktop image to be displayed on both monitors, select the **Use two monitors** check box in the **Monitor management** block. If necessary, you can configure the layout of monitors.

6. If you want to use the Microsoft Remote Desktop Connection Broker to connect to a remote desktop, use the **Remote Desktop Connection Broker collection ID** field to specify the collection ID in the format `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` refers to the specific identifier of the collection).

7. If you want to automatically restore a remote desktop connection that is unexpectedly disconnected, select the **Connect again if connection is lost** check box.

8. Click the back arrow in the upper-right corner of the window to return to the remote desktop connection window.

Configuring settings for connecting to Basis.WorkPlace remote desktops

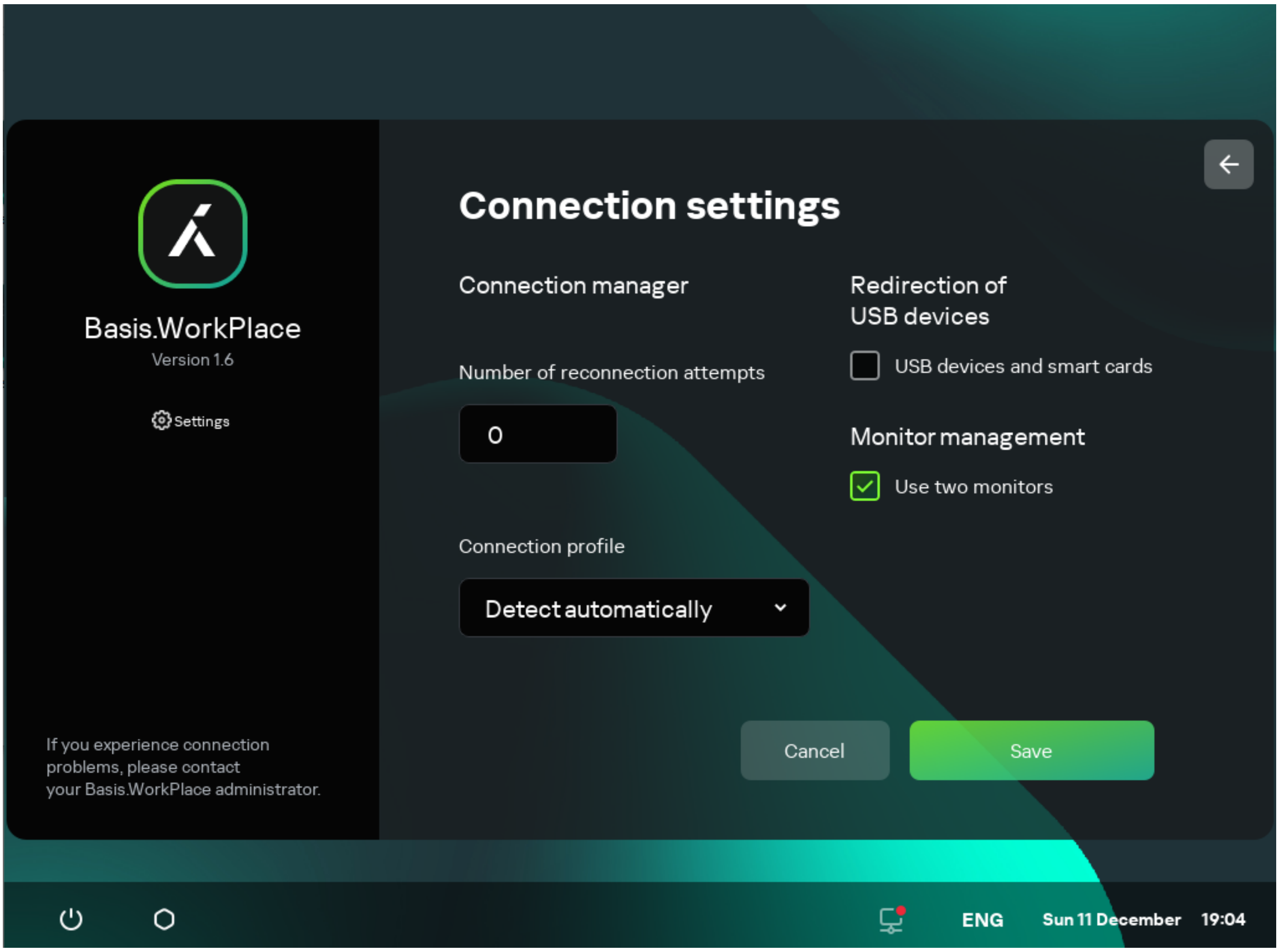
Kaspersky Thin Client lets you configure settings for connecting to remote desktops managed by Basis.WorkPlace.

To configure settings for connecting to remote desktops managed by Basis.WorkPlace:

1. In the main window of Kaspersky Thin Client, click the **Basis.WorkPlace** button.

2. In the remote desktop connection window that opens, click **Settings** in the left part of the window.

This opens a window in which you can configure settings for connecting to a remote desktop (see the figure below).



Basis.WorkPlace
Version 1.6
Settings
If you experience connection problems, please contact your Basis.WorkPlace administrator.
Cancel
Save
ENG
Sun 11 December
19:04

Connection settings

Connection manager

Number of reconnection attempts: 0

Connection profile: Detect automatically

Redirection of USB devices

□ USB devices and smart cards

Monitor management

☑ Use two monitors

Window for configuring settings for connecting to a remote desktop managed by Basis.WorkPlace

3. If you need to enable or disable redirection of USB devices to a remote desktop, select or clear the **USB devices and smart cards** check box in the **Redirection of USB devices** block.

> Redirection of USB devices to a remote desktop managed by Basis.WorkPlace may be blocked by the Basis.WorkPlace administrator.

4. In the **Number of reconnection attempts** field, enter the number of times that Kaspersky Thin Client should attempt to reconnect to the Basis.WorkPlace connection broker if disconnected. You can indicate no more than five attempts at reconnection.

5. In the **Connection profile** drop-down list, select the type of connection between Kaspersky Thin Client and the Basis.WorkPlace connection broker. The type of connection depends on the connection speed. The following values are available:

   - **Detect automatically**
   - **Modem**
   - **Low-speed broadband connection**
   - **Satellite**

- **High-speed broadband connection**
- **Wide area network**
- **Local area network**

6. If two monitors are installed at your workstation and you want a remote desktop image to be displayed on both monitors, select the **Use two monitors** check box in the **Monitor management** block. If necessary, you can configure the layout of monitors.
7. Click **Save** in the lower part of the window to save the changes.
8. Click the back arrow in the upper-right corner of the window to return to the remote desktop connection window.

Managing power-saving mode

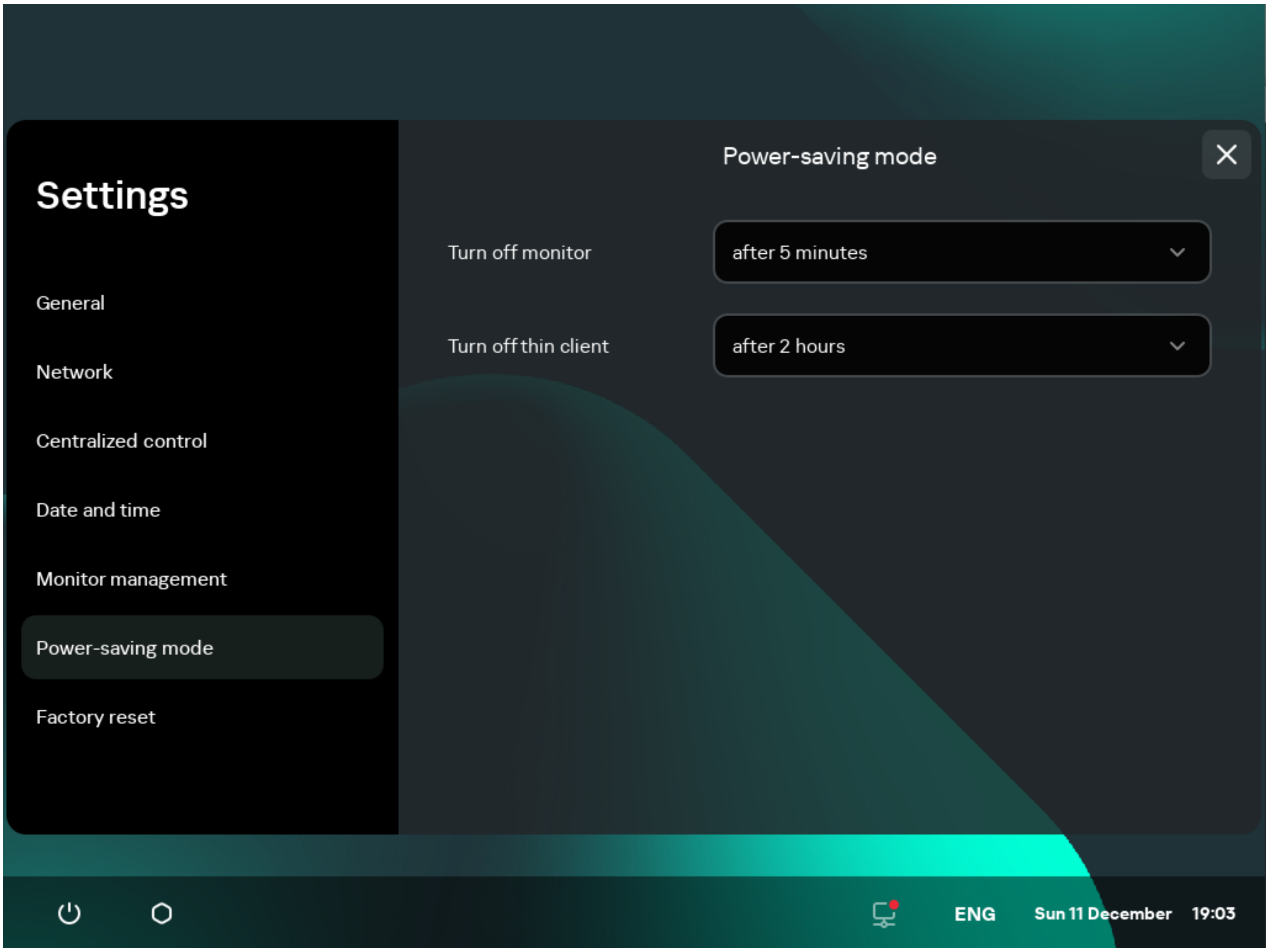
Power-saving mode reduces energy consumption by the device. In this mode, Kaspersky Thin Client continues to operate normally while retaining the active remote desktop connection.

> If Kaspersky Thin Client is a member of an administration group and is controlled centrally through Web Console, and the **Enforced** function is enabled, power-saving mode management is unavailable in the Kaspersky Thin Client interface.

You can configure the time to wait before a monitor is switched to power-saving mode. The monitor will turn on automatically when you click your mouse, press a key on your keyboard, or move your mouse cursor. You can also configure a Kaspersky Thin Client inactivity period after which the thin client will be turned off. To resume operations of the thin client, you will have to turn it on.

To configure power-saving mode:

1. In the Kaspersky Thin Client control panel, click ⬢ and select **Settings** in the menu that opens.
2. In the window that opens, select the **Power-saving mode** section (see the figure below).



Power-saving mode

Turn off monitor: after 5 minutes

Turn off thin client: after 2 hours

Settings. Power-saving mode section

3. In the **Turn off monitor** drop-down list, select the system inactivity period after which the monitor will be switched to power-saving mode.

4. In the **Turn off thin client** drop-down list, select the system inactivity period after which the thin client will be turned off.

You can also configure power-saving mode through the Kaspersky Security Center Web Console interface.

Configuring monitors layout

If two monitors are installed at your workstation, you can select which monitor will be used as the primary monitor and which one will be used as the secondary monitor when showing the remote desktop screen. When connected to the remote desktop, the connection panel is displayed in the upper part of the screen on the primary monitor.

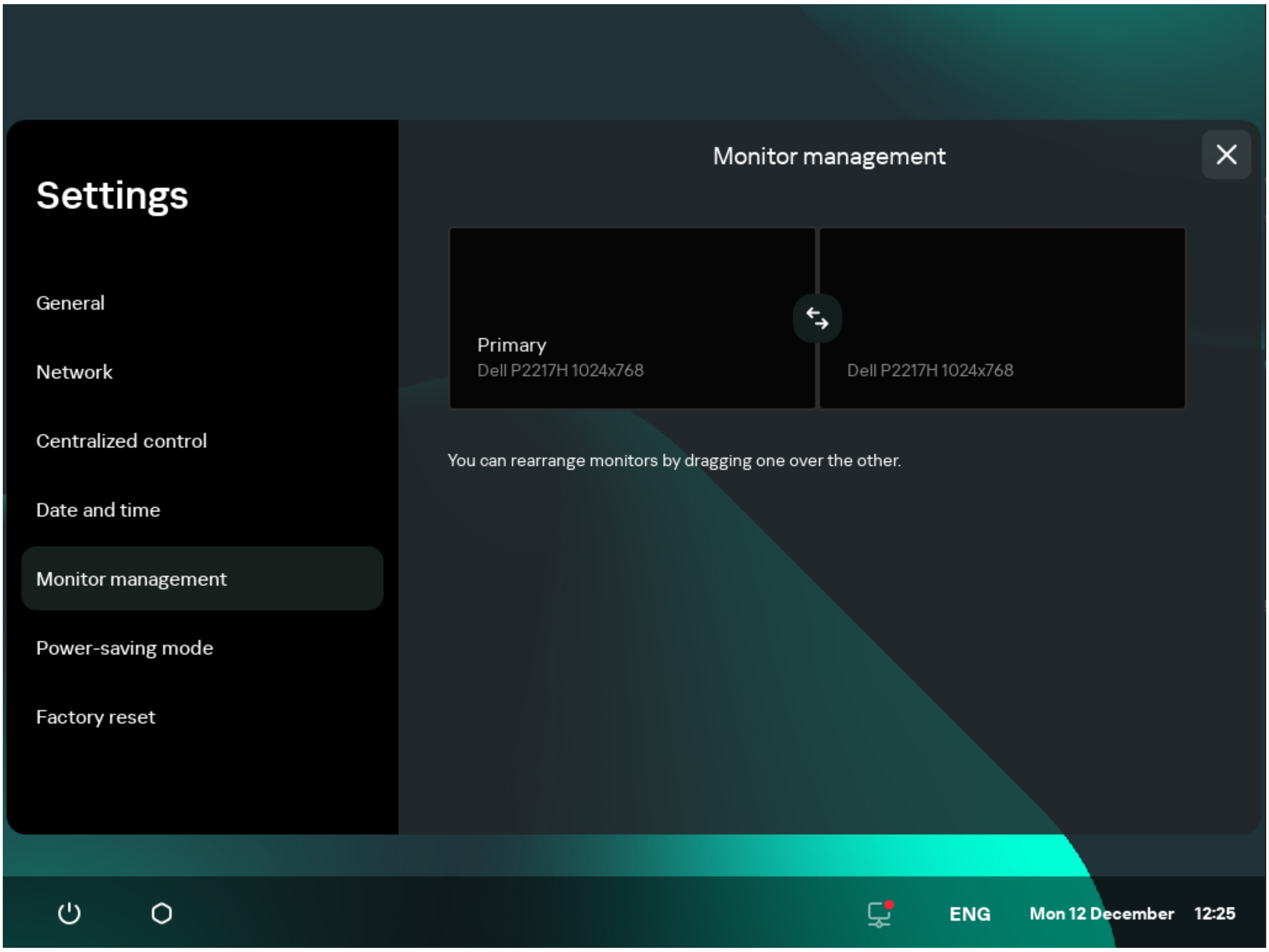
> To use two monitors, you must first enable dual monitors support in the settings for connecting to remote desktops either via RDP or managed by Basis.WorkPlace.

To change the layout of monitors for displaying the remote desktop:

1. In the Kaspersky Thin Client control panel, click ⬡ and select **Settings** in the menu that opens.

2. In the window that opens, select the **Monitor management** section (see the figure below).

The window that opens displays the layout of monitors schematically. The primary monitor is always positioned on the left and labeled.



Settings. **Monitor management** section

3. Change the position of monitors by clicking the ⇆ button located between the monitors on the layout.

The layout of monitors for displaying the remote desktop will be changed.

Managing access to Kaspersky Thin Client settings

You can configure the Kaspersky Thin Client interface to display or hide settings that are configured once and are no longer used in core operating scenarios of the thin client.

Kaspersky Thin Client lets you hide the following system settings simultaneously:

- RDP connection settings
- Basis.WorkPlace connection settings
- General settings
- Network settings
- Kaspersky Security Center connection settings
- Date and time

- Power-saving mode settings
- Layout of monitors
- Reset of Kaspersky Thin Client settings

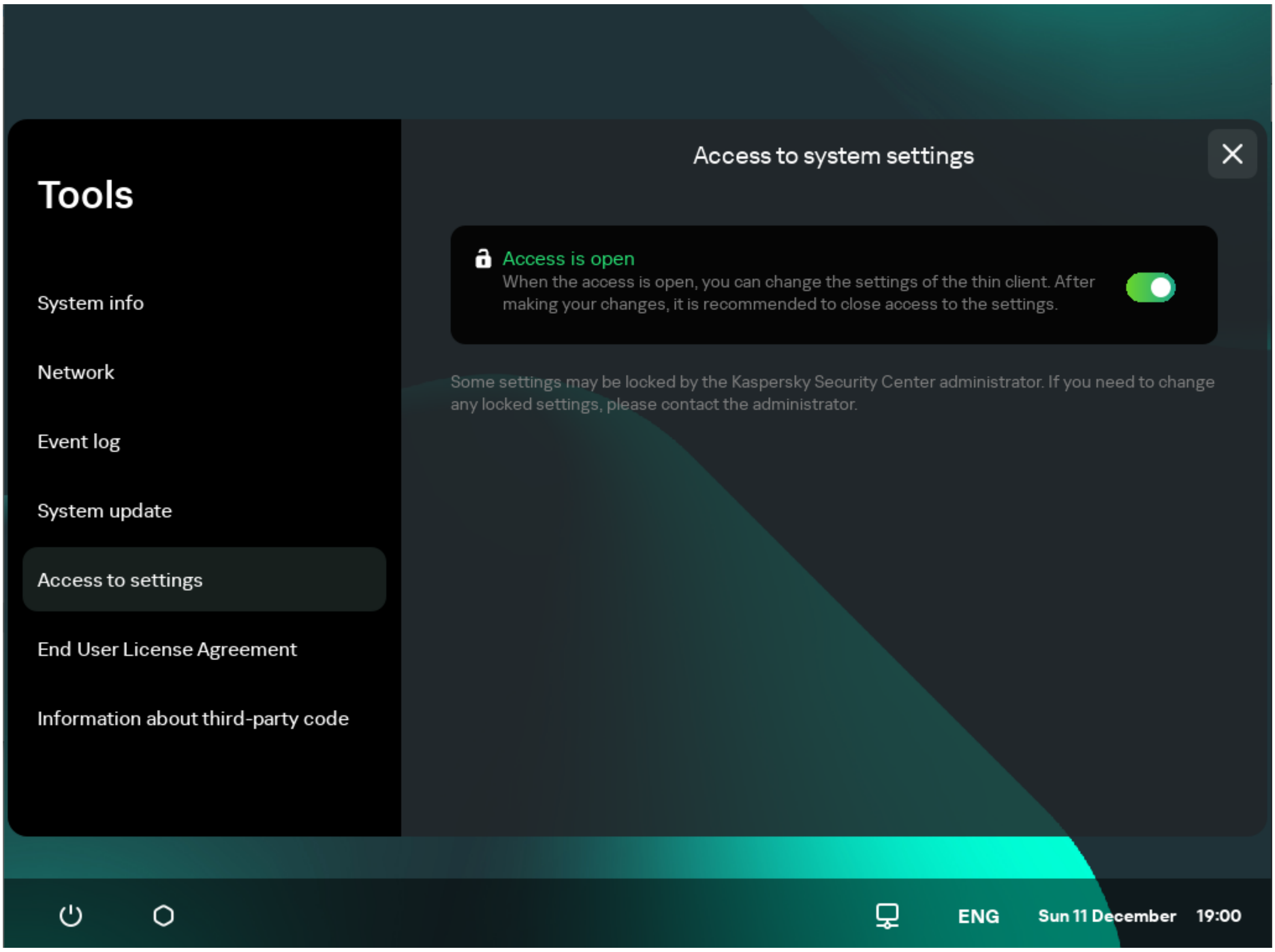
> If Kaspersky Thin Client is a member of an administration group and is controlled centrally through the Web Console, the settings listed above are hidden in the Kaspersky Thin Client interface.

To enable or disable the display of Kaspersky Thin Client settings:

1. In the Kaspersky Thin Client control panel, click ⬡ and select **Tools** in the menu that opens.
2. In the window that opens, select the **Access to settings** section (see the figure below) and do one of the following:
   - If you need to hide the settings, move the toggle button to the **Access is closed** position.

     The settings will be hidden.
   - If you need to display the settings, move the toggle button to the **Access is open** position.

     The settings will be displayed. You will be able to define new values for these settings.



Access to system settings

Access is open

When the access is open, you can change the settings of the thin client. After making your changes, it is recommended to close access to the settings.

Some settings may be locked by the Kaspersky Security Center administrator. If you need to change any locked settings, please contact the administrator.

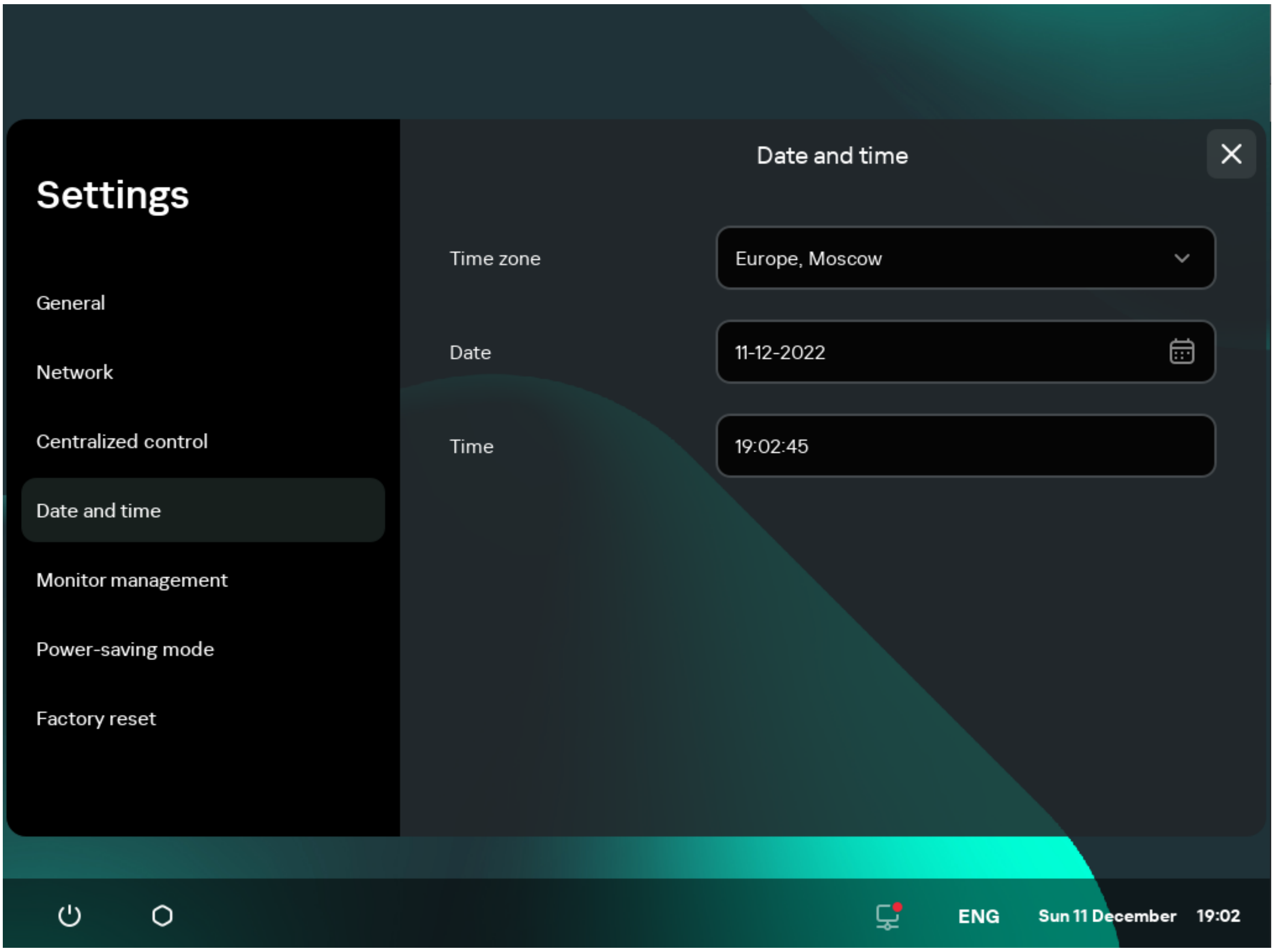
Tools. **Access to settings** section

Configuring the date and time

When Kaspersky Thin Client is connected to Kaspersky Security Center, it receives the date and time from the Kaspersky Security Center Administration Server. You can manually change the date and time of Kaspersky Thin Client only if the system is not being controlled via Kaspersky Security Center.

To change the date and time of Kaspersky Thin Client:

1. In the Kaspersky Thin Client control panel, click ⬡ and select **Settings** in the menu that opens.
2. In the window that opens, select the **Date and time** section (see the figure below).



Time zone: Europe, Moscow

Date: 11-12-2022

Time: 19:02:45

Settings. **Date and time** section

3. Configure the date and time settings:
   - Select the relevant time zone from the **Time zone** drop-down list.
   - Click the **Date** field and use the mouse or keyboard to select the date in the form that opens. To navigate between dates on the calendar using the keyboard, you can use the following keys:
     - **`TAB`** lets you move one month ahead on the calendar.
     - **`SHIFT+TAB`** lets you move one month back on the calendar.
     - The right arrow (→) lets you move one day ahead on the calendar.

    - The left arrow (←) lets you move one day back on the calendar.

- In the **Time** field, enter the current time in `HH:MM:SS` format.

  > If Kaspersky Thin Client is a member of an administration group and is controlled centrally through the Web Console, the **Date** and **Time** fields cannot be changed.

4. Click **Save** in the lower part of the window to save the changes.

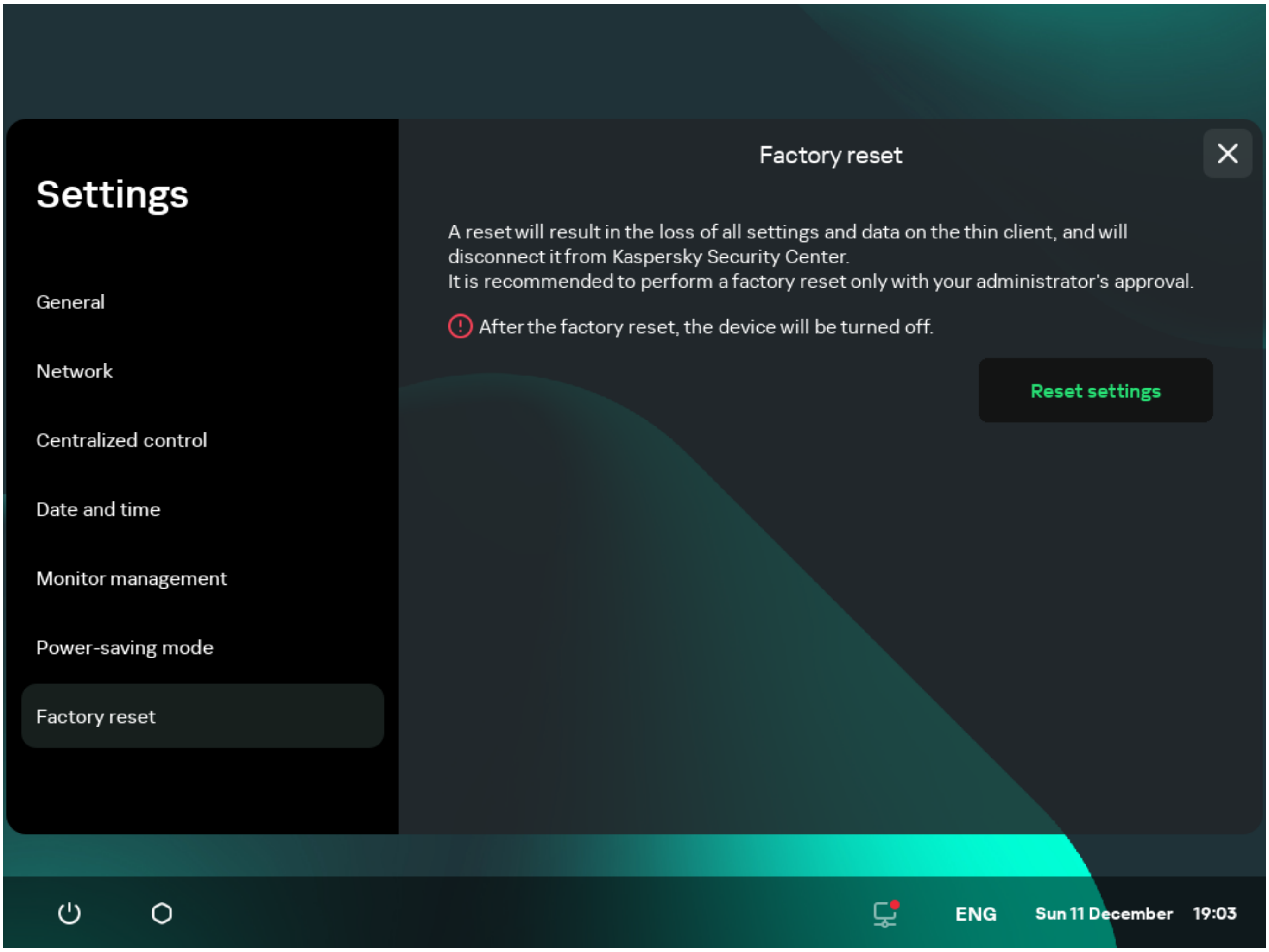
Resetting Kaspersky Thin Client settings

> Reset will result in the loss of all defined settings and all data of Kaspersky Thin Client (except the audit log and system date), and will disconnect the device from Kaspersky Security Center. We recommend performing a reset only after approval with your company administrator.

To reset the settings of Kaspersky Thin Client:

1. In the Kaspersky Thin Client control panel, click ⬡ and select **Settings** in the menu that opens.

2. In the window that opens, select the **Factory reset** section (see the figure below).



A reset will result in the loss of all settings and data on the thin client, and will disconnect it from Kaspersky Security Center.
It is recommended to perform a factory reset only with your administrator's approval.

ⓘ After the factory reset, the device will be turned off.

Settings. **Factory reset** section

3. In the window that opens, click the **Reset settings** button.

   This opens the **Confirm reset** window showing a confirmation code.

4. Provide the confirmation code to the Kaspersky Security Center administrator. The administrator contact details are provided in the **Confirm reset** window. The Kaspersky Security Center administrator sends you a confirmation code in response.

5. Click **Next**.

6. In the **Confirmation code** window that opens, enter the code provided by the Kaspersky Security Center administrator and click the **Confirm** button.

As a result, all defined settings of Kaspersky Thin Client will be restored to their original values (default), all data on the device will be deleted (except the audit log and system date), and Kaspersky Thin Client will be disconnected from Kaspersky Security Center. After reset, the thin client turns off.

Working with Kaspersky Thin Client

The main scenario for working with Kaspersky Thin Client involves preparing the system before startup, starting the system, and connecting it to a remote desktop. Once you are finished working with the remote desktop, the connection session is supposed to be closed, and the system turned off. You spend the rest of the time in a familiar software environment and do not need to interact with the Kaspersky Thin Client interface.

The main operating scenario for working with Kaspersky Thin Client consists of the following steps:

1. **Preparing Kaspersky Thin Client for startup**

   Connect a monitor, keyboard, and mouse to the device before starting it for the first time. If necessary, you can also connect USB devices and/or USB tokens.

2. **Starting Kaspersky Thin Client**

   Turn on the thin client to get started.

3. **Connecting to a remote desktop**

   Connect to a remote desktop and start working.

4. **Locking the desktop and resuming operations**

   If you need to temporarily leave your workstation, lock your remote desktop. Resume operations when you return to your workstation. For detailed information about locking the remote desktop and resuming operations, see the manual of the operating system you are connecting to remotely.

5. **Closing a connection session**

   Close the remote desktop connection session when you are finished working with it.

6. **Stopping Kaspersky Thin Client**

   Turn off the thin client at the end of the workday.

Connecting to a remote desktop

Kaspersky Thin Client lets you choose to either directly connect to a remote desktop via RDP or connect to remote desktops managed by Basis.WorkPlace. Depending on the infrastructure in your enterprise, you can select one of the following options:

- **Connecting to a remote desktop via RDP** ?

The following specifics must be taken into consideration when connecting to a remote desktop via RDP:

- When connecting to a remote desktop running an Astra Linux operating system (CE or SE) using the xRDP protocol, an expired user password is accepted, but the connection fails. The same applies to using an incorrect user name. Also, there is no way to change the password given such a connection.
- You cannot connect to a remote desktop running a Microsoft Windows operating system with Network Layer Authentication (NLA) enabled if the password has expired. Also, you cannot change the password by yourself given such a connection.

  To solve these issues, we recommend contacting your enterprise administrator.

To connect to a remote desktop via RDP:

1. Turn on Kaspersky Thin Client.
2. In the main window of Kaspersky Thin Client, click the **RDP** button.
3. In the connection window that opens, specify the settings for connecting to the remote desktop:
   a. In the **Server** field, specify the IP address or name of the RDP server to which you want to connect.

      > If a Wallix Bastion privileged user access control system is deployed in your enterprise infrastructure, you can connect to remote desktops through this system by indicating its IP address or server name in the **Server** field.

      Kaspersky Thin Client saves the address of the last RDP server with which a connection was successfully established, so you do not need to enter it again when reconnecting.

   b. In the **User name** field, enter the local or domain user name. If you indicate a domain user name, you are not required to indicate the name of the domain. However, you can do so in `Domain\User name` format.

      Kaspersky Thin Client saves the user name that last successfully connected to the RDP server, so you do not need to enter it again when reconnecting.

   c. In the **Password** field, enter the user password.

      The user password is cleared each time you exit the remote desktop connection window.
4. Press the **ENTER** key or click the **Connect** button.

   If you are connecting to a remote desktop for the first time and Kaspersky Thin Client is not included in an administration group, check the settings of the added certificate in the opened **Adding certificate** window and click the **Add certificate** button.

   If Kaspersky Thin Client was previously added to an administration group that is managed through the Kaspersky Security Center Web Console and the Kaspersky Security Center administrator added an RDP server authentication certificate for this administration group, the connection is established automatically.

   The certificate for authenticating the RDP server will be added to the system certificate store of Kaspersky Thin Client and will be used for subsequent connections.
5. If you specified the Remote Desktop Connection Broker collection ID when configuring a remote desktop connection and multiple desktops are available to you, in the remote desktop selection window that opens, click the button with the name of the desktop to which you want to connect.

After a few seconds, the monitor will show the remote desktop of the computer that you are connected to via RDP.

You can also configure RDP connection settings by clicking **Settings**.

- Connecting to a remote desktop managed by Basis.WorkPlace ?

When working with Kaspersky Thin Client via Basis.WorkPlace, the following limitations apply:

- Users cannot be authorized with smart cards in the Basis.WorkPlace connection manager.
- Users cannot initiate a password change in Kaspersky Thin Client.
- Simultaneous connection to multiple remote desktops managed by Basis.WorkPlace is not supported.

The Basis.WorkPlace administrator can restrict access to desktops managed by Basis.WorkPlace. For example, the administrator can lock your user account or block access to remote desktops managed by Basis.WorkPlace that were previously available to your user account. If you encounter any problems connecting to a remote desktop, we recommend contacting your Basis.WorkPlace administrator.

To connect to a remote desktop managed by Basis.WorkPlace:

1. Turn on Kaspersky Thin Client.
2. In the main window of Kaspersky Thin Client, click the **Basis.WorkPlace** button.
3. In the connection window that opens, specify the Basis.WorkPlace connection settings:
   a. In the **Server** field, specify the IP address or name of the Basis.WorkPlace connection manager server.

      Kaspersky Thin Client saves the address of the Basis.WorkPlace connection manager with which a connection was successfully established, so you do not need to enter it again when reconnecting.

   b. In the **Domain** field, enter the domain name.

   c. In the **User name** field, enter the user name.

      Kaspersky Thin Client saves the user name that last successfully connected to Basis.WorkPlace, so you do not need to enter it again when reconnecting.

   d. In the **Password** field, enter the user password.

      The password is cleared each time you exit the window for connecting to desktops managed by Basis.WorkPlace.

      > If the number of allowed incorrect password entry attempts is exceeded, the user account will be blocked. The corresponding message will be displayed in the remote desktop connection window. The number of allowed password entry attempts is defined by the active security policy set by the Basis.WorkPlace administrator.

4. Click the **Connect** button.

   If you are connecting to a remote desktop managed by Basis.WorkPlace for the first time and Kaspersky Thin Client is not included in an administration group, check the settings of the added certificate in the opened **Adding certificate** window and click the **Add certificate** button.

   If Kaspersky Thin Client was previously added to an administration group that is managed through the Kaspersky Security Center Web Console and the Kaspersky Security Center administrator added a certificate for authenticating the Basis.WorkPlace connection broker for this administration group, the connection to a remote desktop managed by Basis.WorkPlace is established automatically.

   The certificate for authenticating the Basis.WorkPlace connection broker will be added to the system certificate store of Kaspersky Thin Client and will be used for subsequent connections.

   A window for selecting a remote desktop opens showing all desktops that are available for connection.

5. If you need to refresh the list of desktops, click the **Reload** button.

6. Click the button with the name of the desktop to which you want to connect.

   After a few seconds, the monitor will show the remote desktop to which you are connected.

In the window for connecting to desktops managed by Basis.WorkPlace, you can also configure the connection settings by clicking **Settings**.

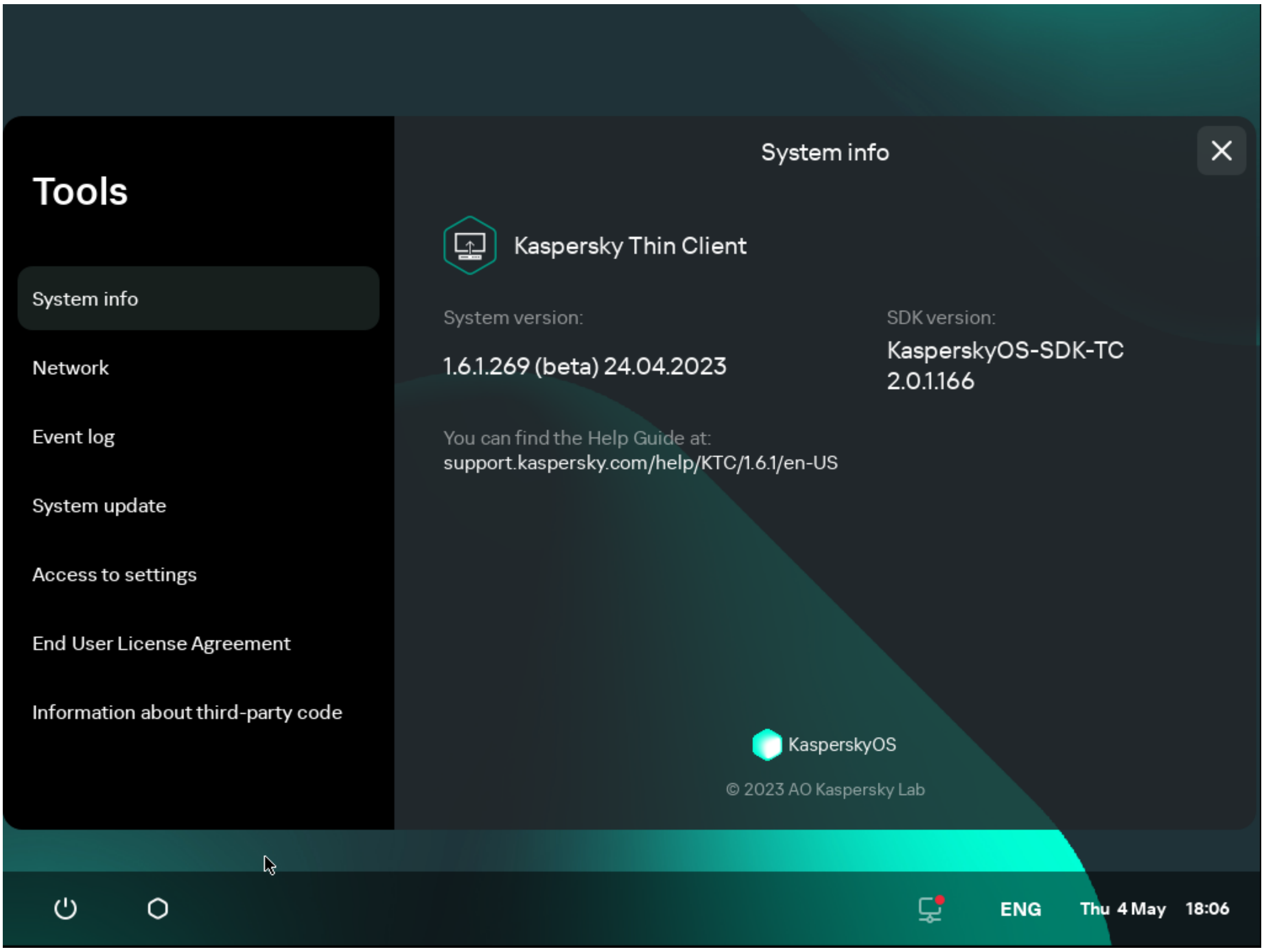
When connecting to a remote desktop, Kaspersky Thin Client uses TLS encryption to protect the connection session and protect data from interception or falsification.

Viewing information about Kaspersky Thin Client

You can view information about Kaspersky Thin Client under **Tools** → **System info**.

The **System info** section (see the figure below) shows the following data:

- Kaspersky Thin Client version number
- KasperskyOS version number
- Link to the Kaspersky Thin Client Online Help



System info

Kaspersky Thin Client

System version:
1.6.1.269 (beta) 24.04.2023

SDK version:
KasperskyOS-SDK-TC 2.0.1.166

You can find the Help Guide at:
support.kaspersky.com/help/KTC/1.6.1/en-US

KasperskyOS

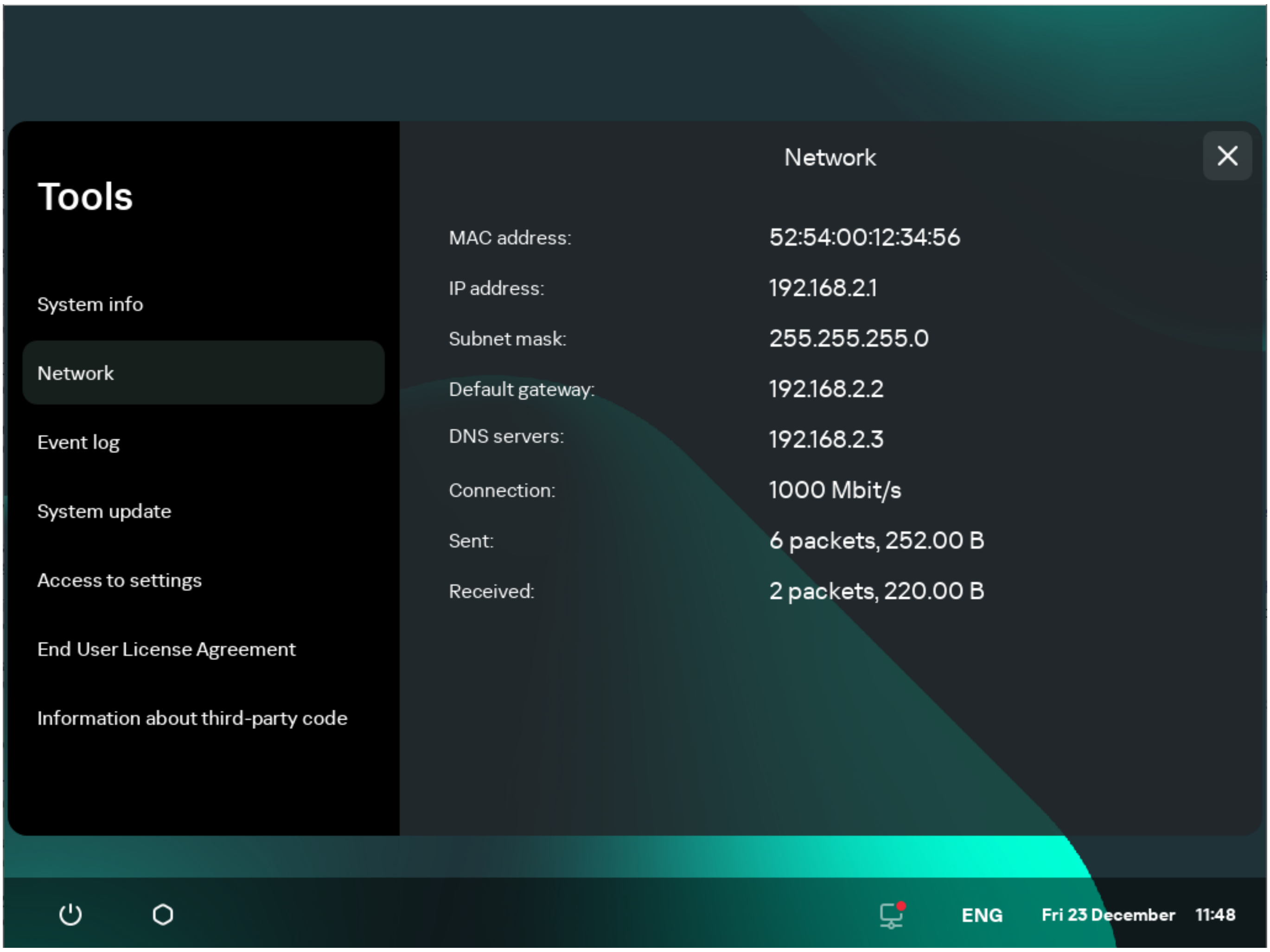
© 2023 AO Kaspersky Lab

Viewing network status information

You can view Kaspersky Thin Client network connection settings and network status under **Tools** → **Network**. Information about Kaspersky Thin Client network connection settings is updated automatically at least once every second.

The **Network** section displays the following information about the settings for connecting Kaspersky Thin Client to the network (see the figure below):

- **MAC address**: MAC address of the device where Kaspersky Thin Client is installed.
- **IP address**: IP address of the device where Kaspersky Thin Client is installed.
- **Subnet mask**: subnet mask that contains the IP address of the device.
- **Default gateway**: address of the network gateway.
- **DNS servers**: addresses of DNS servers. To view all addresses (if there are more than three), hover the mouse over the setting value.
- **Connection**: status of the network connection of Kaspersky Thin Client and the connection speed.
- **Sent**: number and total size of network packets sent from Kaspersky Thin Client.
- **Received**: number and total size of network packets received by Kaspersky Thin Client.



Network

MAC address:	52:54:00:12:34:56
IP address:	192.168.2.1
Subnet mask:	255.255.255.0
Default gateway:	192.168.2.2
DNS servers:	192.168.2.3
Connection:	1000 Mbit/s
Sent:	6 packets, 252.00 B
Received:	2 packets, 220.00 B

Tools. **Network** section

Managing Kaspersky Thin Client logs

This section provides information about working with Kaspersky Thin Client logs.

About Kaspersky Thin Client logs

Kaspersky Thin Client maintains two types of logs:

- Event log. This log saves all events registered by Kaspersky Thin Client components. You can view the event log in the Kaspersky Thin Client interface, and forward it to a log server.
- Audit log. This log stores data on the certificates uploaded to Kaspersky Thin Client, and contains information on instances when Kaspersky Security Center was used to enable or disable management of thin clients. The audit log cannot be viewed in the Kaspersky Thin Client interface. You can forward the audit log file to a log server.

The Kaspersky Thin Client event log contains the following information:

- Date and time when the event occurred.
- Name of the Kaspersky Thin Client component that registered the event.

- Event severity. The following values are possible:
  - *Trace* is all possible messages and warnings that occur during application operation.
  - *Debug* is debug messages and all informational and important messages, and all warnings and messages about common and critical errors.
  - *Info* is informational messages, important messages and all warnings, and messages about common and critical errors.
  - *Warn* is all warnings and messages about ordinary and critical errors.
  - *Error* is messages about errors and critical errors in application operation.
  - *Fatal* is messages about critical errors in application operation.
- Debug information in <File>:<Line Number>,<Function> format, where:
  - File means file name.
  - Line Number is number of the line in the file.
  - Function is debug information.
- Process ID and thread ID.
- Product version ID.

The Kaspersky Thin Client audit log contains the following information:

- Upload date and time of the certificate for connecting Kaspersky Thin Client to Kaspersky Security Center.
- Address of the Kaspersky Security Center Administration Server (IP address and/or domain server name).
- Kaspersky Security Center Administration Server port number.
- List of certificate attributes: issuer name, subject name, certificate fingerprint, validity start date and time, validity end date and time, thin client ID.
- Information about incidents when management of Kaspersky Thin Client via the Kaspersky Security Center Web Console was enabled or disabled.

Forwarding of event and audit logs

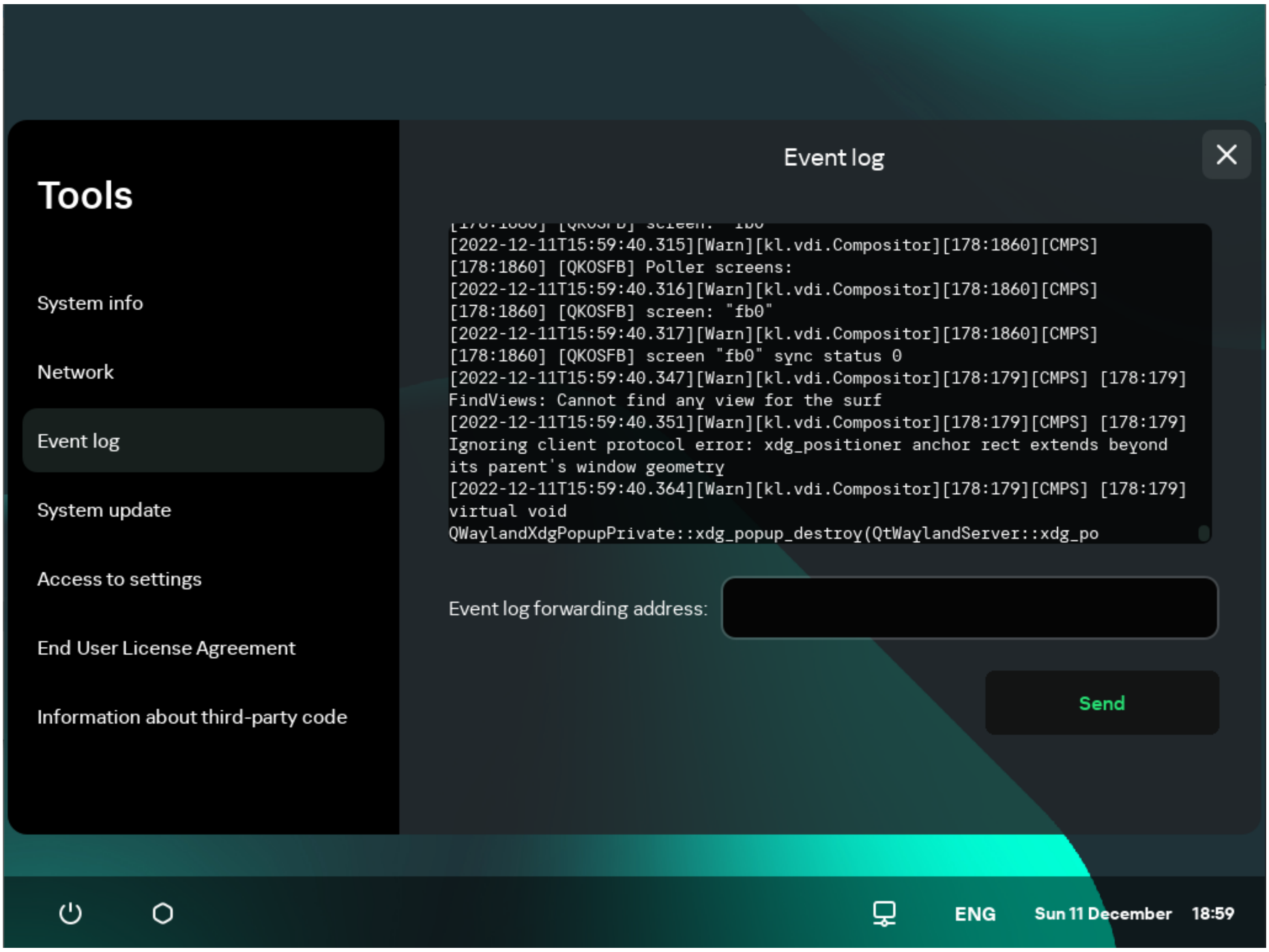
You can view the Kaspersky Thin Client event log through the Kaspersky Thin Client interface under **Tools** → **Event log**. You can also forward the event log to a log server. The audit log is automatically sent to the server together with the event log.

To forward Kaspersky Thin Client audit and event logs to a log server, a log server must first be deployed in your enterprise infrastructure. For detailed information on server deployment, please refer to the Administrator's Guide for this server.

The maximum file sizes for the event log and audit log are 150 MB and 512 MB, respectively. When the file size of event or audit logs reaches its corresponding limit, Kaspersky Thin Client deletes the existing logs and starts to record new ones. Each time event and audit logs are updated, the current version of Kaspersky Thin Client is recorded at the beginning of the log.

To forward Kaspersky Thin Client audit and event logs:

1. In the Kaspersky Thin Client control panel, click ⬡ and select **Tools** in the menu that opens.
2. In the window that opens, select the **Event log** section (see the figure below).



```
[178:1860] [QKOSFB] screen: "fb0"
[2022-12-11T15:59:40.315][Warn][kl.vdi.Compositor][178:1860][CMPS]
[178:1860] [QKOSFB] Poller screens:
[2022-12-11T15:59:40.316][Warn][kl.vdi.Compositor][178:1860][CMPS]
[178:1860] [QKOSFB] screen: "fb0"
[2022-12-11T15:59:40.317][Warn][kl.vdi.Compositor][178:1860][CMPS]
[178:1860] [QKOSFB] screen "fb0" sync status 0
[2022-12-11T15:59:40.347][Warn][kl.vdi.Compositor][178:179][CMPS] [178:179]
FindViews: Cannot find any view for the surf
[2022-12-11T15:59:40.351][Warn][kl.vdi.Compositor][178:179][CMPS] [178:179]
Ignoring client protocol error: xdg_positioner anchor rect extends beyond
its parent's window geometry
[2022-12-11T15:59:40.364][Warn][kl.vdi.Compositor][178:179][CMPS] [178:179]
virtual void
QWaylandXdgPopupPrivate::xdg_popup_destroy(QtWaylandServer::xdg_po
```

Tools. **Event log** section

This displays information about registered events of Kaspersky Thin Client.

3. In the **Event log forwarding address** field, enter the address of the destination server that should receive audit and event logs, and click the **Send** button.

   If Kaspersky Thin Client is a member of an administration group and is centrally controlled through the Web Console, and the **Enforced** function is enabled, the **Event log forwarding address** field will contain the value set by the Kaspersky Security Center administrator that cannot be changed.

   We recommend verifying the correct address of the destination server to which you are sending logs. If the wrong address is indicated, logs could be sent to unauthorized third parties. If this is the case, the confidentiality of the data they contain could be compromised.

4. In the window that opens, confirm that you want to forward audit and event logs.

If Kaspersky Thin Client is not in an administration group and you are forwarding audit and event logs to a log server for the first time, check the settings of the certificate being added in the opened **Adding certificate** window and click the **Add certificate** button. The certificate will be added to the system certificate store of Kaspersky Thin Client and will be used for subsequent connections.

Kaspersky Thin Client audit and event logs will be forwarded to the specified server.

Updating Kaspersky Thin Client

Kaspersky Thin Client can be updated only if the thin client is connected to Kaspersky Security Center.

Kaspersky Thin Client cannot be updated from version 1.5/1.6 to version 1.6.1 beta.

Available updates are downloaded to the thin client from the Kaspersky Security Center Administration Server or from Kaspersky update servers only after Kaspersky Security Center administrator approves these updates in the Web Console interface. If a new End User License Agreement is generated for the new Kaspersky Thin Client version, Kaspersky Security Center administrator accepts it in the Kaspersky Security Center Web Console interface. For detailed information on approving updates by the administrator, refer to the *Approving and declining software updates* section of the Kaspersky Security Center Online Help Guide. Additionally, Kaspersky Security Center administrator can configure regular checks for Kaspersky Thin Client updates (for details, refer to the *Scenario: Regular updating Kaspersky databases and applications* section of the Kaspersky Security Center Online Help Guide).

After the updates are downloaded to the device, the Kaspersky Thin Client interface displays a notification with the time when the update will be applied.

You can install an update in one of the following ways:

- **Directly from the notification about the available update**

  - If you want to install the update right now, click the **Restart now** button in the available update notification window.

    The updates will be installed, and Kaspersky Thin Client will restart.

  - If you want to install the updates later, click **Later** in the available update notification window. The update notification shows how long the update will be postponed for. The time of the postponed startup of the update is set by the administrator.

    The system restart and update will be postponed.

    If you ignore or close the Kaspersky Thin Client update notification several times, the update will be installed automatically.

- **When restarting or turning off the thin client**

1. In the Kaspersky Thin Client control panel, click the shutdown button ⏻.

2. Depending on whether you plan to quit or continue working with Kaspersky Thin Client after the update, do one of the following:

   - If you want to continue working, select **Update and restart** in the menu that opens.

     The updates will be installed, and Kaspersky Thin Client will restart.

   - If you want to quit working, select **Update and shut down** in the menu that opens.

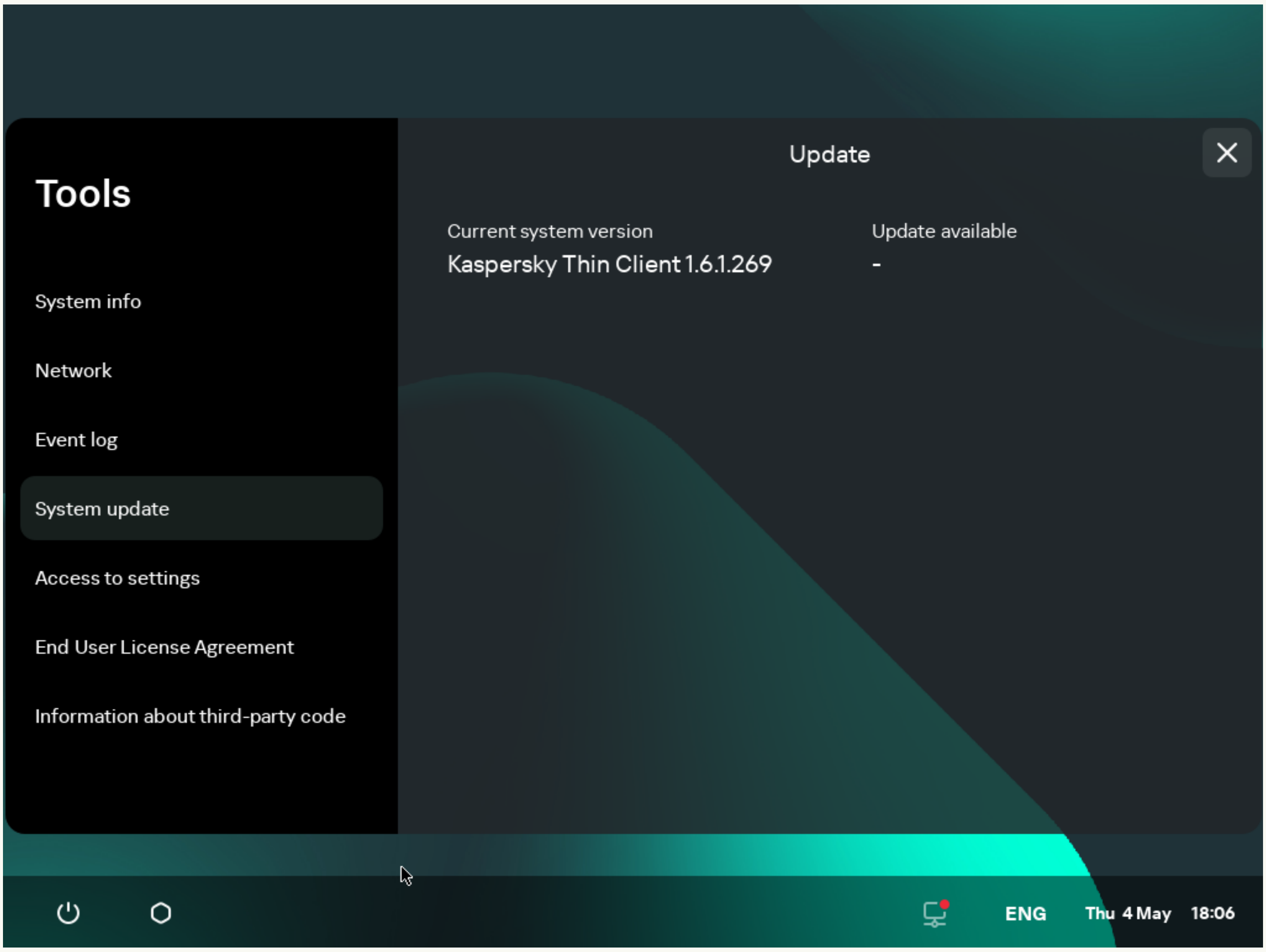
     The updates will be installed, and Kaspersky Thin Client will shut down.

- In the System update section

1. In the Kaspersky Thin Client control panel, click ⬡ and select **Tools** in the menu that opens.

2. Select the **System update** section.

   A window opens, displaying information about the current system version and downloaded updates (see the figure below).



Current system version
Kaspersky Thin Client 1.6.1.269

Update available
-

Tools. **System update** section

3. Click **Install and restart**. If no updates are available, the button is not displayed.

The updates will be installed, and Kaspersky Thin Client will restart.

If a Kaspersky Thin Client update has been downloaded but you have not yet restarted, the update will be installed automatically during the next restart or shutdown of the device.

Closing a connection session

To close a remote desktop connection session:

1. Click the Kaspersky Thin Client connection panel in the center of the upper part of the remote desktop.
2. In the connection panel that expands, click the **Disconnect from server** button.

   As a result, the desktop connection session will be closed and the monitor will show the remote desktop connection window.

If the Basis.WorkPlace administrator has set an idle timeout period for Kaspersky Thin Client that terminates the connection session with a remote desktop managed by Basis.WorkPlace, this connection will be closed automatically when the session is idle for this period of time.

Managing Kaspersky Thin Client using hotkeys

You can use dedicated hotkeys and key combinations when working with Kaspersky Thin Client and when connecting to a remote desktop. The table below lists all the available hotkeys and key combinations.

Hotkeys and key combinations for Kaspersky Thin Client

Keys and key combinations	Action	Scope
`Win`	Open or close the shutdown menu.	Any window of the Kaspersky Thin Client interface that displays the control panel.
→ ←	Switch between the available remote desktop connection options: **RDP**, **Basis.WorkPlace**.	Main window of the Kaspersky Thin Client.
↑ ↓	- Switch between drop-down list items. - Scroll page content up or down.	Any window of the Kaspersky Thin Client interface that contains a field with a drop-down list or is scrollable as its content is larger than the window size.
`Tab`	Switch between the following items: - Remote desktop connection options: **RDP**, **Basis.WorkPlace**. - The sequence of fields, for example, in the **Settings** window. You can switch between the items in the following directions: *left to right* and *top to bottom*.	- Main window of the Kaspersky Thin Client. - Any window of the Kaspersky Thin Client interface that contains several fields. When you switch between the items, unavailable items (for example, disabled fields) and inactive items are skipped.
`Shift+Tab`	Switch between the following items: - Remote desktop connection options: **RDP**, **Basis.WorkPlace**. - The sequence of fields, for example, in the **Settings** window.	- Main window of the Kaspersky Thin Client. - Any window of the Kaspersky Thin Client interface that contains several fields. When you switch between the items, unavailable items (for example, disabled fields) and inactive items are skipped.

	You can switch between the items in the following directions: *right to left* and *bottom to top*.	
`Space` or `Enter`	Click the button.	Button.
`Space` or `Enter`	Open or close the drop-down list.	Drop-down list. When you switch between the list items, unavailable and inactive items are skipped.
`Esc`	Close a window.	Any window that can be closed.
`Esc`	Collapse the connection panel.	During a remote desktop connection when hovering the mouse over the connection panel.
`Alt`+`Shift`	Change the keyboard language.	Any window of the Kaspersky Thin Client interface.
`Alt`+`Page down`	Move to the next section of the **Settings** or **Tools** window.	The **Settings** or **Tools** window. When you switch between the sections, their state and the element in focus are preserved. For example, in the **Settings** window, when you switch from the **General** section to the **Network** section, the focus in the **General** section remains in the same field where it was when you switched to another section.
`Alt`+`Page up`	Move to the previous section of the **Settings** or **Tools** window.	The **Settings** or **Tools** window. When you switch between the sections, their state and the element in focus are preserved. For example, in the **Settings** window, when you switch from the **General** section to the **Network** section, the focus in the **General** section remains in the same field where it was when you switched to another section.
`Ctrl`+`Alt`+`Home`	Collapse or restore the connection panel.	During a remote desktop connection.
`Ctrl`+`D`	Disconnect from the remote desktop.	During a remote desktop connection when hovering the mouse over the connection panel.
`Win`+`I`	Open **Settings** if access to settings is enabled.	Any window of the Kaspersky Thin Client interface.
`Win`+`U`	Open **Tools**.	Any window of the Kaspersky Thin Client interface.
`Win`+`Esc`	Turn off Kaspersky	Any window of the Kaspersky Thin Client interface.

	Thin Client.	
`Win`+**`F12`** or **`Win`**+**`End`**	Restart Kaspersky Thin Client.	Any window of the Kaspersky Thin Client interface.

Managing Kaspersky Thin Client through the Kaspersky Security Center Web Console

The Kaspersky Security Center Web Console (hereinafter also referred to as simply "the Web Console") is a web application designed to let you centrally perform the main tasks for managing and maintaining the security system of an enterprise network. The Web Console is a Kaspersky Security Center component that provides a user interface. For detailed information about the Kaspersky Security Center Web Console, please refer to the Kaspersky Security Center Web Console Online Help Guide ↗.

About the Kaspersky Security Management Suite web plug-in

The *Kaspersky Security Management Suite web plug-in* (hereinafter also referred to as "the web plug-in") is a specialized component that provides the capability to manage the operation of Kaspersky Thin Client through the Kaspersky Security Center Web Console. The web plug-in is included in the Kaspersky Thin Client distribution kit and facilitates interaction between Kaspersky Thin Client and Kaspersky Security Center.

The web plug-in lets you centrally perform the following operations:

- Manage Kaspersky Thin Client settings.
- Receive and view Kaspersky Thin Client events.
- Manage security certificates of Kaspersky Thin Client.

To enable interaction between Kaspersky Thin Client and Kaspersky Security Center, the following conditions must be met:

- When configuring Kaspersky Thin Client, you must specify the settings for connecting to Kaspersky Security Center.
- In the Kaspersky Security Center Web Console, you must install the Kaspersky Security Management Suite web plug-in.

Installing the Kaspersky Security Management Suite web plug-in

The Kaspersky Security Management Suite web plug-in is not installed in the Web Console by default. The web plug-in is included in the Kaspersky Thin Client distribution kit and must be installed on the computer that has the Kaspersky Security Center Web Console installed. You can view the list of installed web plug-ins in the Web Console interface (**Console settings** → **Web plug-ins**). Web plug-in functions are available to all administrators that have access to the Web Console in a browser, and you can restrict access to Kaspersky Security Management Suite functionality.

> If you plan to use the default port to connect the thin client to Kaspersky Security Center, port 13292 must be available on the Kaspersky Security Center Administration Server. If you plan to use a port other than 13292, you must set the permissions accordingly. For details on port enabling on a Kaspersky Security Center Administration Server, see the *Modifying the Mobile Device Management settings* ↗ section of the Kaspersky Security Center Online Help Guide.

Kaspersky Security Center and the Kaspersky Security Center Web Console are not included in the Kaspersky Thin Client distribution kit. They must be installed separately.

To install the web plug-in in the Web Console:

1. In the menu of the Web Console, select **Console settings** → **Web plug-ins**.

   A list of available Web Console management plug-ins is displayed.

2. Click the **Add from file** button.

3. In the panel that opens on the right, add the following files:

   - ZIP archive containing the web plug-in distribution package (plugin.zip) provided in the Kaspersky Thin Client distribution kit by clicking the **Upload ZIP file** button.

   - Signature file (signature.txt) provided in the Kaspersky Thin Client distribution kit by clicking the **Upload signature** button.

4. Click on the **Add** button.

5. Please carefully read and accept the End User License Agreement.

6. When installation of the web plug-in is complete, click **OK**.

The Kaspersky Security Management Suite web plug-in will be loaded in the default configuration and will appear in the list of Web Console management plug-ins.

Updating the Kaspersky Security Management Suite web plug-in

The Kaspersky Security Management Suite web plug-in can be updated only to a newer version.

You must first obtain the ZIP archive containing the distribution package for the new version of the web plug-in and the digital signature of the archive from Kaspersky experts.

To update the web plug-in in the Web Console:

1. In the menu of the Web Console, select **Console settings** → **Web plug-ins**.

2. In the displayed list of Web Console plug-ins, find Kaspersky Security Management Suite and click it.

3. In the window that opens, click the **Update from file** button.

4. In the panel that opens on the right, add the following files:

   - ZIP archive containing the plug-in distribution package by clicking the **Upload ZIP file** button

   - Digital signature file by clicking the **Upload signature** button

5. Click **Update**.

6. If a new End User License Agreement was created for the latest version of the plug-in, please carefully read and accept the new End User License Agreement.

7. After the update is complete and you see a message confirming successful installation of the update, click **OK**.

The Kaspersky Security Management Suite web plug-in will be updated, and its version information and update time will be displayed in the table of plug-ins in the Web Console.

Removing the Kaspersky Security Management Suite web plug-in

The Kaspersky Security Management Suite web plug-in can be removed from the Web Console. After the web plug-in is removed, you will not be able to manage Kaspersky Thin Client through the Web Console interface.

To remove the Kaspersky Security Management Suite web plug-in from the Web Console:

1. In the menu of the Web Console interface, select **Console settings** → **Web plug-ins**.

   A list of available Web Console management plug-ins is displayed.

2. In the list of management plug-ins, select the check box next to the Kaspersky Security Management Suite web plug-in.

3. Click the **Delete** button.

4. In the plug-in removal confirmation window that opens, do one of the following:

   - If you need to save a backup copy of the plug-in, click **OK**.

     A backup copy of the plug-in will be created. The Kaspersky Security Management Suite web plug-in will be removed from the Web Console.

   - If you do not need to save a backup copy of the plug-in, click the **Skip backup** button.

     The Kaspersky Security Management Suite web plug-in will be removed from the Web Console.

5. In the window containing information about plug-in removal that opens, click **OK**.

Restricting access to functions of the Kaspersky Security Management Suite web plug-in

If a Kaspersky Security Center user is not granted sufficient rights to access application functions, or the standard Kaspersky Security Center role is not assigned, the user cannot work in Kaspersky Security Center Web Console.

You can configure Kaspersky Security Center user rights to access application functions in the following ways:

- Configure rights of each user or user group separately.

- Create standard Kaspersky Security Center roles with preconfigured sets of rights and assign these roles to users depending on their duties.

A *role* is a preconfigured set of rights to access Kaspersky Security Management Suite functions, which you can assign to users. We recommend configuring role access rights according to typical tasks and duties of users. Once a user has been assigned a role, they gain access to the functions they require to fulfill their duties.

For details on configuring role-based access, see the *Configuring access rights to application features. Role-based access control* section of the Kaspersky Security Center Online Help Guide.

In addition to the standard Kaspersky Security Center roles, you can also assign users the following standard roles for managing Kaspersky Thin Client functions:

- *Security Officer*. This role has permissions to view all sections of Kaspersky Security Management Suite and to manage Kaspersky Thin Client certificates. You can assign this role to an employee in charge of the information security in your enterprise.
- *Administrator*. This role has permissions to view all sections of Kaspersky Security Management Suite and manage remote desktop connection settings, general settings, system settings, and Kaspersky Thin Client data. You can assign this role to an employee responsible for supporting and administering information systems in your organization.
- *Advanced administrator*. This role has permissions to view and manage all sections of Kaspersky Security Management Suite and manage certificates, remote desktop connection settings, general settings, system settings, and Kaspersky Thin Client data. You can assign this role to an employee who is responsible for supporting and administering information systems in your organization, and is in charge of the information security in your organization.

The table below describes the functions available to a user depending on their assigned role for managing Kaspersky Thin Client. For functions marked with the ✓ icon, the corresponding Kaspersky Thin Client settings can be changed through the Web Console. All roles can view the Kaspersky Thin Client settings pertaining to all functions through the Web Console.

Kaspersky Thin Client management functions available in the Web Console depending on the user role

Function	Security Officer	Administrator	Advanced administrator
Managing certificates in a Kaspersky Security Management Suite policy	✓	–	✓
Configuring settings for connecting to remote desktops in a Kaspersky Security Management Suite policy	–	✓	✓
Configuring general settings in a Kaspersky Security Management Suite policy	–	✓	✓
Managing system settings in a Kaspersky Security Management Suite policy	–	✓	✓
Managing Kaspersky Thin Client data in a Kaspersky Security Management Suite policy	–	✓	✓

Logging in and out of the Web Console

To log in to the Web Console, you need to ask the administrator for the web address of the Kaspersky Security Center Administration Server and the port number that were specified during installation (port 8080 is used by default). You must also enable JavaScript in your browser.

To log in to the Web Console:

1. In your browser, go to `https://<Administration Server address>:<Port number>`. For the Kaspersky Security Center Web Console browser requirements, please refer to the *Hardware and software requirements* section of the Kaspersky Security Center Web Console Online Help Guide.

   The login page opens.

2. Log in using the user name and password of a local administrator.

   If the Administration Server does not respond or you entered incorrect account credentials, an error message will be displayed.

After logging in, the Dashboard appears displaying the last language and theme that were used. If you are logging in to the Web Console for the first time, the Quick Start Wizard starts. For additional information about how the Kaspersky Security Center Web Console works, please refer to the Kaspersky Security Center Web Console Online Help Guide.

To log out of the Web Console:

1. In the lower-right corner of the screen, click the user name.

2. In the menu that opens, select **Sign out**.

The Web Console closes, and the login page is displayed.

Adding Kaspersky Thin Client to a group of managed devices

You must add Kaspersky Thin Client to a group of managed devices when connecting it to the Web Console for the first time.

To add Kaspersky Thin Client to a group of managed devices:

1. In the main window of the Web Console, select **Discovery & deployment** → **Unassigned devices**.

   The list of all detected unassigned devices will be displayed.

2. Select the check box next to the name of the device that you want to add to the group of managed devices.

3. Click the **Move to group** button.

   The **Move to group** panel opens on the right. Select the check box next to the **Managed devices** administration group.

4. Click the **Move** button.

Kaspersky Thin Client will be added to the group of managed devices of the Web Console.

Managing policies

A *policy* is a collection of Kaspersky Thin Client operating settings defined for an administration group. You can configure multiple policies with different values for one device. For different administration groups, the settings of the application may be different. Each administration group can create its own policy for the application. For more detailed information on using Kaspersky Security Center policies to manage the application, please refer to the *Policies and policy profiles* section of the Kaspersky Security Center Online Help Guide.

Policy settings are configured in the Kaspersky Security Center Web Console by using the web plug-in and are transmitted to Kaspersky Thin Client when the application synchronizes with Kaspersky Security Center. The synchronization period can be changed in the policy settings.

Active and inactive policy

A policy is intended for a group of managed devices and can be active or inactive. The settings of an active policy are saved on client devices during synchronization. You cannot simultaneously apply multiple policies to one device, therefore only one policy can be active in each group.

You can create an unlimited number of inactive policies. An inactive policy does not affect application settings on devices in the network. Inactive policies are intended as preparations for emergency situations, such as a virus attack. If there is an attack via flash drives, you can activate a policy that blocks access to flash drives. In this case, the active policy automatically becomes inactive.

Settings inheritance

Policies, like administration groups, have a hierarchy. By default, a child policy inherits the settings from the parent policy. A *child policy* is a policy for nested hierarchy levels. In other words, it is a policy for nested administration groups and secondary Administration Servers. You can turn off inheritance of settings from the parent policy.

Each policy setting has the 🔒 attribute, which indicates if the settings can be modified in policies or in the local application settings. Depending on the status of this attribute, one of the following values is displayed next to a setting:

- 🔓 Undefined ○ **Undefined**. If an open lock icon is displayed next to a setting and the toggle button is disabled, this setting is not defined in the policy. A user can change these settings in the local interface of the Kaspersky application. These settings are referred to as unlocked.
- 🔒 Enforced ● **Enforced**. If a closed lock icon is displayed next to a setting and the toggle button is enabled, this setting is applied to devices on which the policy is applied. A user cannot change the values of these settings in the local interface of the Kaspersky application. These settings are referred to as locked.

The 🔒 attribute applies for a child policy only if inheritance of the parent policy settings is enabled for the child policy.

Policy creation

To manage a group of devices running Kaspersky Thin Client through the Web Console, you must create a policy.

To create a policy for a group of devices:

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.
2. Click on the **Add** button.
3. From the list of applications in the window that opens, select Kaspersky Security Management Suite and click **Next**.
4. In the new policy configuration window, on the **General** tab, specify the following settings:

- In the **Name** field, enter the policy name. By default, the field displays the Kaspersky Thin Client management web plug-in name as Kaspersky Security Management Suite.
- In the **Policy status** block, select one of the following statuses: *Active*, *Inactive*, *Out-of-office*. The default status is *Active*.
- If you need to configure inheritance of policy settings, configure the following settings in the **Settings inheritance** block:
  - Enable or disable the **Inherit settings from parent policy** option.
  - Enable or disable the **Force inheritance of settings in child policies** option.

5. Click the **Save** button in the lower part of the page.

   The policy will be created and will appear in the list of policies of the Web Console.

Editing a policy

You can edit a previously created policy for a group of devices running Kaspersky Thin Client.

To change a policy:

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.
2. Select the policy that you need to edit.
3. In the policy configuration window that opens, define the following settings on the **General** tab:
   - If necessary, enter a new policy name in the **Name** field.
   - If you need to change the policy status, use the **Policy status** block to select one of the following statuses: *Active*, *Inactive*, *Out-of-office*.
   - If you need to configure inheritance of policy settings, configure the following settings in the **Settings inheritance** block:
     - Enable or disable the **Inherit settings from parent policy** option.
     - Enable or disable the **Force inheritance of settings in child policies** option.
4. Click the **Save** button in the lower part of the page.

   The changes made to the policy will be saved and displayed in the policy properties in the **Revision history** section.

Configuring Kaspersky Thin Client settings through the Web Console

This section contains information about configuring Kaspersky Thin Client settings through the Web Console.

Configuring general settings of Kaspersky Thin Client through the Web Console

In the Web Console, you can configure general settings for one device or for a group of devices running Kaspersky Thin Client.

How to configure general settings for one device ?

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device where Kaspersky Thin Client is running. You can view the device name in the control panel of the Kaspersky Thin Client interface. If the computer name is not on the list, add it to the Managed devices group. You can also manage devices that have not yet been added to the managed devices group by selecting **Discovery & deployment** → **Unassigned devices**.

   > If a managed device is added to an administration group and an enforced policy is configured for the settings of this group, the settings that were individually configured for this device will not be applied.

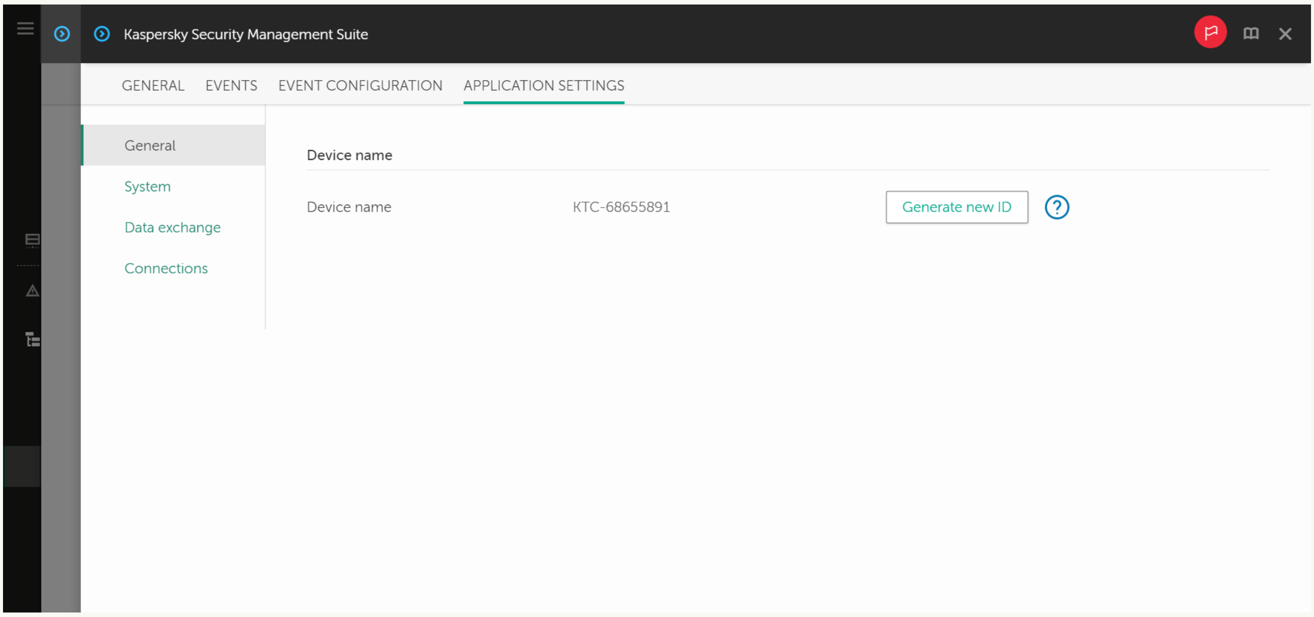
3. In the window that opens, select the **Applications** tab.

4. Click the name of the Kaspersky Security Management Suite web plug-in.

   This opens a window containing information about Kaspersky Thin Client.

5. Select the **Application settings** tab.

6. Select the **General** section (see the figure below).



Kaspersky Security Management Suite

GENERAL EVENTS EVENT CONFIGURATION APPLICATION SETTINGS

General
System
Data exchange
Connections

Device name

Device name KTC-68655891 Generate new ID

Window for configuring general settings through the Web Console for one device

7. If you need to change the ID in the thin client name, click the **Generate new ID** button in the **Device name** block. The managed device for which you want to generate a new ID must be added to an administration group, and this group must have a configured and enforced policy for a group device naming rule.

   The new ID in the thin client name will be created after the device is synchronized with Kaspersky Security Center.

8. Click **Save** in the lower part of the window to save the changes.

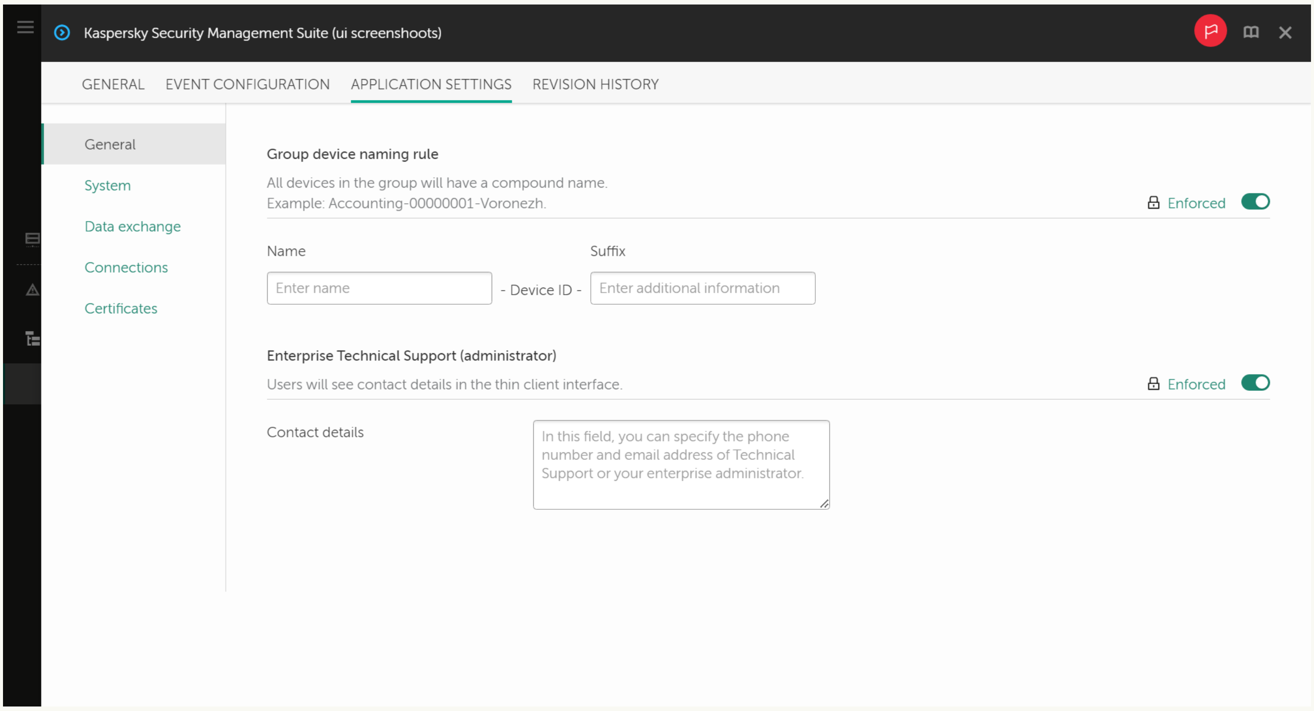
How to configure general settings for a group of devices

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name for the Kaspersky Security Management Suite web plug-in.

3. In the window that opens, select the **Application settings** tab.

4. Select the **General** section (see the figure below).



Group device naming rule

All devices in the group will have a compound name.
Example: Accounting-00000001-Voronezh.

🔒 Enforced ●

Name: Enter name - Device ID - Suffix: Enter additional information

Enterprise Technical Support (administrator)

Users will see contact details in the thin client interface.

🔒 Enforced ●

Contact details: In this field, you can specify the phone number and email address of Technical Support or your enterprise administrator.

Window for configuring general settings through the Web Console for a group of devices

5. If you need to specify a new name format for administration group devices, use the **Group device naming rule** block to indicate the new group name and additional information. You can use uppercase and lowercase letters of the Latin and Cyrillic alphabets, and special characters. A unique ID (eight characters) will be automatically generated for each device in the group. The number of characters in the device name must not exceed 30 characters.

6. Move the toggle button located on the right in the **Group device naming rule** block to the **Enforced** position.

> If the toggle button next to the name of a group of settings is in the **Enforced** position (🔒 Enforced ●), the defined values of these settings are applied to devices on which the policy is applied, and these settings cannot be changed in the Kaspersky Thin Client interface. If the toggle button next to the name of a group of settings is in the **Undefined** position (🔒 Undefined ○), the defined values of these settings are not applied to devices on which the policy is applied, and these settings can be changed for managed devices in the Kaspersky Thin Client interface under **Devices** → **Managed devices**.

7. Add the contact details of the Kaspersky Security Center administrator in the **Contact details** field. You can specify the last name, first name, phone number and email address of the administrator. The number of characters in this field must not exceed 80 characters.

   The contact details of the Kaspersky Security Center administrator are visible to the user in the main window of Kaspersky Thin Client, in the windows for confirming a reset of Kaspersky Thin Client settings and data and confirming changes to Kaspersky Security Center connection settings, and when the certificate for connecting to Kaspersky Security Center is replaced.

8. Move the toggle button located on the right in the **Enterprise Technical Support (administrator)** block to the **Enforced** position.

9. Click **Save** in the lower part of the window to save the changes.

Configuring settings for connecting to a remote desktop via RDP through the Web Console

You can use the Web Console to configure settings for connecting to remote desktops via RDP for one device or group of devices running Kaspersky Thin Client.

How to configure settings for connecting to remote desktops via RDP for one device

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device where Kaspersky Thin Client is running. You can view the device name in the control panel of the Kaspersky Thin Client interface. If the computer name is not on the list, add it to the **Managed devices** group. You can also manage devices that have not yet been added to the managed devices group by selecting **Discovery & deployment** → **Unassigned devices**.

   If a managed device is added to an administration group and an enforced policy is configured for the settings of this group, the settings that were individually configured for this device will not be applied.

3. In the window that opens, select the **Applications** tab.

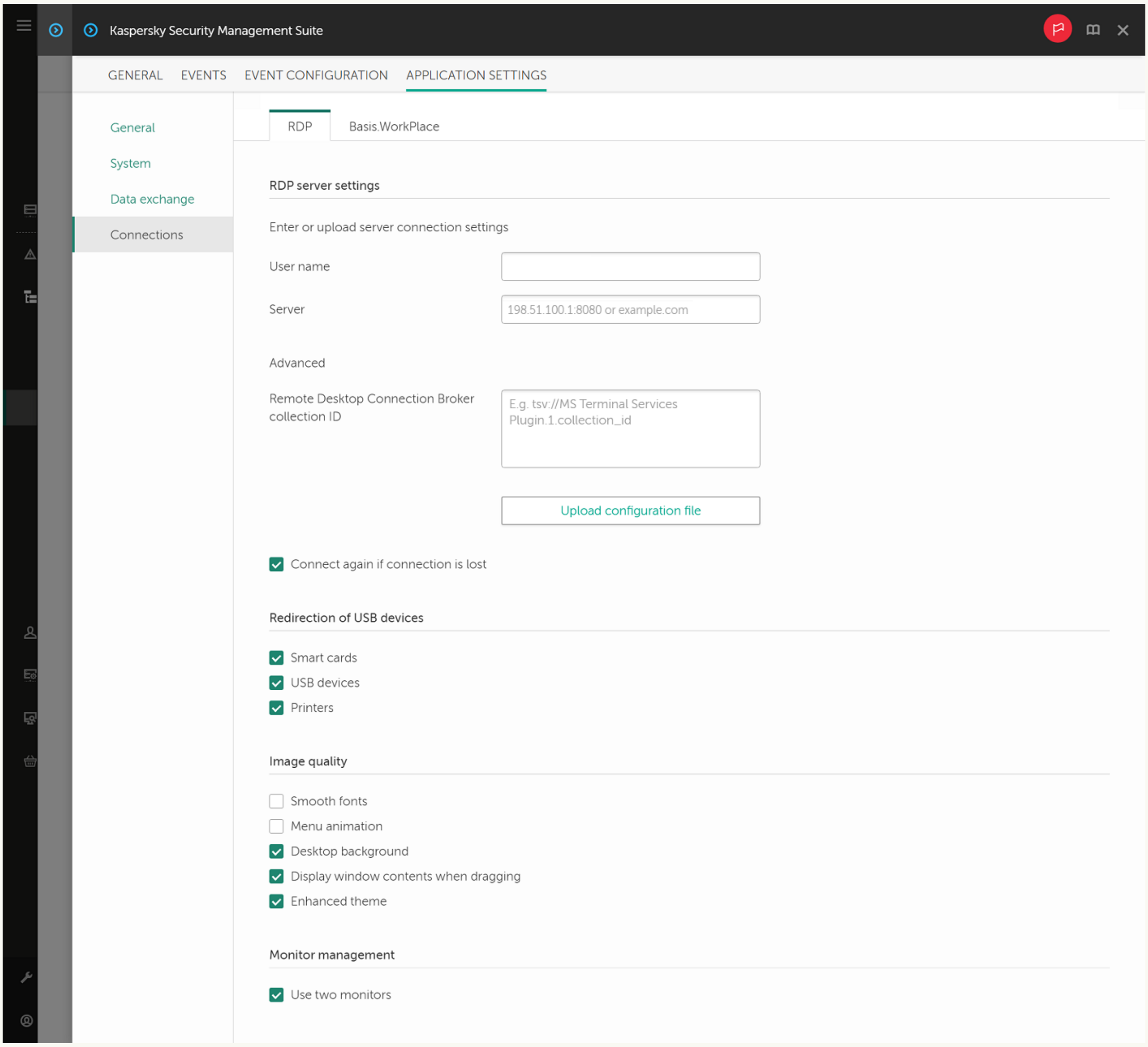
4. Click the name of the Kaspersky Security Management Suite web plug-in.

   This opens a window containing information about Kaspersky Thin Client.

5. Select the **Application settings** tab.

6. Select **Connections** → **RDP**.

   This opens a window in which you can configure settings for connecting to a remote desktop via RDP (see the figure below).



RDP server settings

Enter or upload server connection settings

User name

Server: 198.51.100.1:8080 or example.com

Advanced

Remote Desktop Connection Broker collection ID: E.g. tsv://MS Terminal Services Plugin.1.collection_id

Upload configuration file

☑ Connect again if connection is lost

Redirection of USB devices

☑ Smart cards
☑ USB devices
☑ Printers

Image quality

□ Smooth fonts
□ Menu animation
☑ Desktop background
☑ Display window contents when dragging
☑ Enhanced theme

Monitor management

☑ Use two monitors

Window for configuring settings for connecting to a remote desktop via RDP through the Web Console for one device

7. In the **Server** field, enter the IP address or server name for connecting to a remote desktop via RDP.

8. In the **User name** field, enter the name of the user account that will be used to connect to the remote desktop via RDP.

9. If you want to use the Microsoft Remote Desktop Connection Broker to connect to a remote desktop, use the **Remote Desktop Connection Broker collection ID** field to specify the collection ID in the format `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` refers to the specific identifier of the collection).

   If you have a configuration file containing the settings for connecting to the Microsoft Remote Desktop Connection Broker, upload the file by clicking the **Upload configuration file** button. In this case, you do not have to complete the **Remote Desktop Connection Broker collection ID** field.

10. If you want to automatically restore a remote desktop connection that is unexpectedly disconnected, select the **Connect again if connection is lost** check box.

11. In the **Redirection of USB devices** settings block, select the relevant check boxes next to the devices connected to the thin client via USB that you need to pass through to the remote desktop:

    - **Smart cards** if you want to enable redirection of smart cards and tokens.

    - **USB devices** if you want to enable redirection of USB devices.

    - **Printers** if you want to enable redirection of printers. The remote computer must have the installed driver for the printer that is connected to the thin client.

      All the check boxes are cleared by default.

12. In the **Image quality** block, select the check boxes next to the remote desktop graphics settings that you need to use:

    - **Smooth fonts**

    - **Menu animation**

    - **Desktop background**

    - **Display window contents when dragging**

    - **Enhanced theme**

    Enabling remote desktop display settings may affect the speed of Kaspersky Thin Client operations.

13. If two monitors are installed at your workstation and you want a remote desktop image to be displayed on both monitors, select the **Use two monitors** check box in the **Monitor management** block.

14. Click **Save** in the lower part of the window to save the changes.

How to configure settings for connecting to remote desktops via RDP for a group of devices

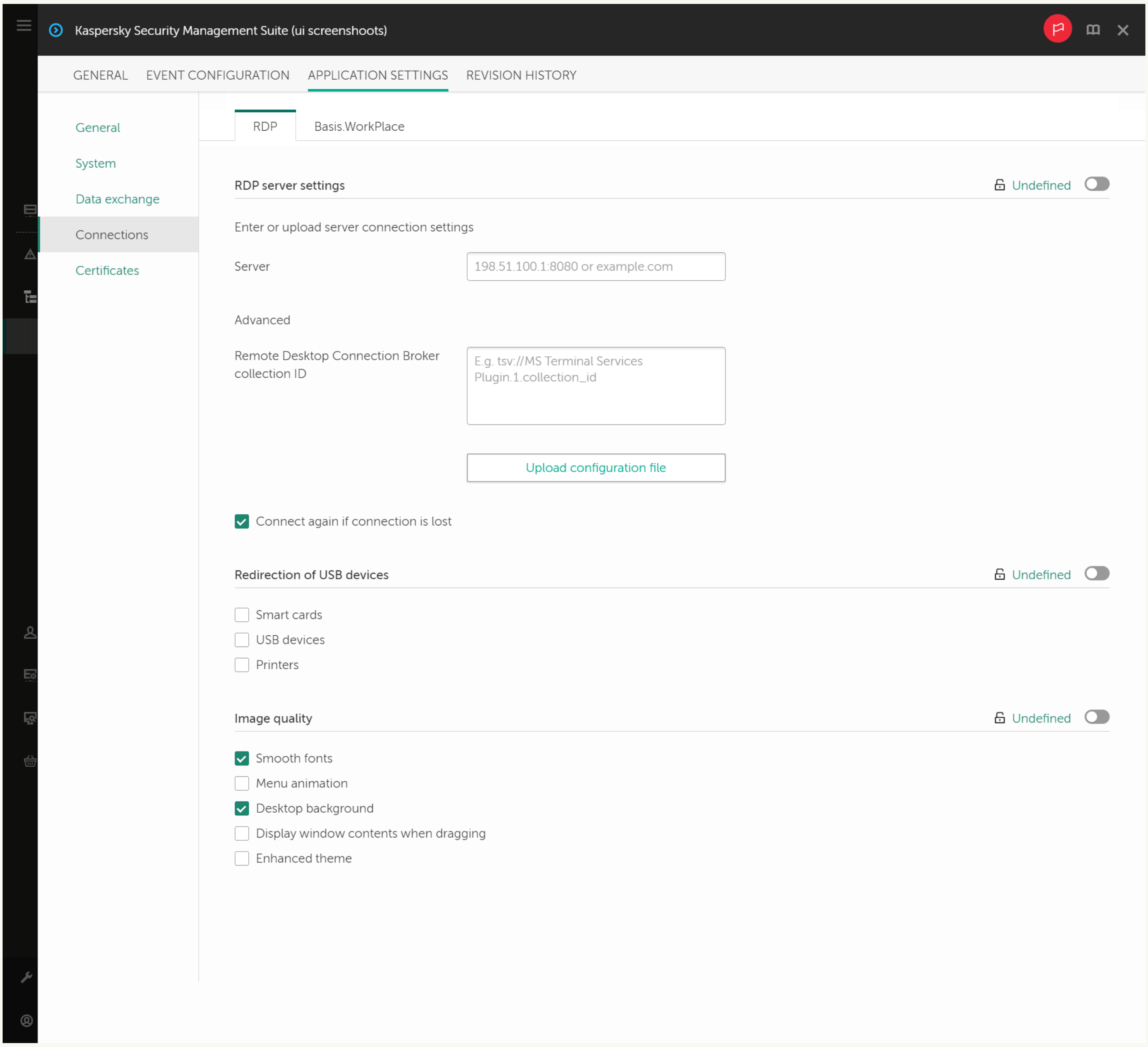
1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name for the Kaspersky Security Management Suite web plug-in.

3. In the window that opens, select the **Application settings** tab.

4. Select **Connections** → **RDP**.

   This opens a window in which you can configure settings for connecting to a remote desktop via RDP (see the figure below).



Kaspersky Security Management Suite (ui screenshots)

GENERAL EVENT CONFIGURATION APPLICATION SETTINGS REVISION HISTORY

General
System
Data exchange
Connections
Certificates

RDP Basis.WorkPlace

RDP server settings — Undefined

Enter or upload server connection settings

Server: 198.51.100.1:8080 or example.com

Advanced

Remote Desktop Connection Broker collection ID: E.g. tsv://MS Terminal Services Plugin.1.collection_id

Upload configuration file

☑ Connect again if connection is lost

Redirection of USB devices — Undefined

□ Smart cards
□ USB devices
□ Printers

Image quality — Undefined

☑ Smooth fonts
□ Menu animation
☑ Desktop background
□ Display window contents when dragging
□ Enhanced theme

Window for configuring settings for connecting to a remote desktop via RDP through the Web Console for a group of devices

5. In the **Server** field, enter the IP address or server name for connecting to a remote desktop via RDP.

6. In the **User name** field, enter the name of the user account that will be used to connect to the remote desktop via RDP.

7. If you want to use the Microsoft Remote Desktop Connection Broker to connect to a remote desktop, use the **Remote Desktop Connection Broker collection ID** field to specify the collection ID in the format `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` refers to the specific identifier of the collection).

If you have a configuration file containing the settings for connecting to the Microsoft Remote Desktop Connection Broker, upload the file by clicking the **Upload configuration file** button. In this case, you do not have to complete the **Remote Desktop Connection Broker collection ID** field.

8. If you want to automatically restore a remote desktop connection that is unexpectedly disconnected, select the **Connect again if connection is lost** check box.

9. In the **Redirection of USB devices** settings block, select the relevant check boxes next to the devices connected to the thin client via USB that you need to pass through to the remote desktop:

   - **Smart cards** if you want to enable redirection of smart cards and tokens.

   - **USB devices** if you want to enable redirection of USB devices.

   - **Printers** if you want to enable redirection of printers. The remote computer must have the installed driver for the printer that is connected to the thin client.

     All the check boxes are cleared by default.

10. In the **Image quality** block, select the check boxes next to the remote desktop graphics settings that you need to use:

    - **Smooth fonts**

    - **Menu animation**

    - **Desktop background**

    - **Display window contents when dragging**

    - **Enhanced theme**

    > Enabling remote desktop display settings may affect the speed of Kaspersky Thin Client operations.

11. Click **Save** in the lower part of the window to save the changes.

> If the toggle button next to the name of a group of settings is in the **Enforced** position (🔒 Enforced ●), the defined values of these settings are applied to devices on which the policy is applied, and these settings cannot be changed in the Kaspersky Thin Client interface. If the toggle button next to the name of a group of settings is in the **Undefined** position (🔓 Undefined ○), the defined values of these settings are not applied to devices on which the policy is applied, and these settings can be changed for managed devices in the Kaspersky Thin Client interface under **Devices** → **Managed devices**.

Configuring settings for connecting to a remote desktop managed by Basis.WorkPlace through the Web Console

You can use the Web Console to configure settings for connecting to a remote desktop managed by Basis.WorkPlace for one device or group of devices running Kaspersky Thin Client.

How to configure settings for connecting to a remote desktop managed by Basis.WorkPlace for one device

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device where Kaspersky Thin Client is running. You can view the device name in the control panel of the Kaspersky Thin Client interface. If the computer name is not on the list, add it to the Managed devices group. You can also manage devices that have not yet been added to the managed devices group by selecting **Discovery & deployment** → **Unassigned devices**.

   If a managed device is added to an administration group and an enforced policy is configured for the settings of this group, the settings that were individually configured for this device will not be applied.

3. In the window that opens, select the **Applications** tab.

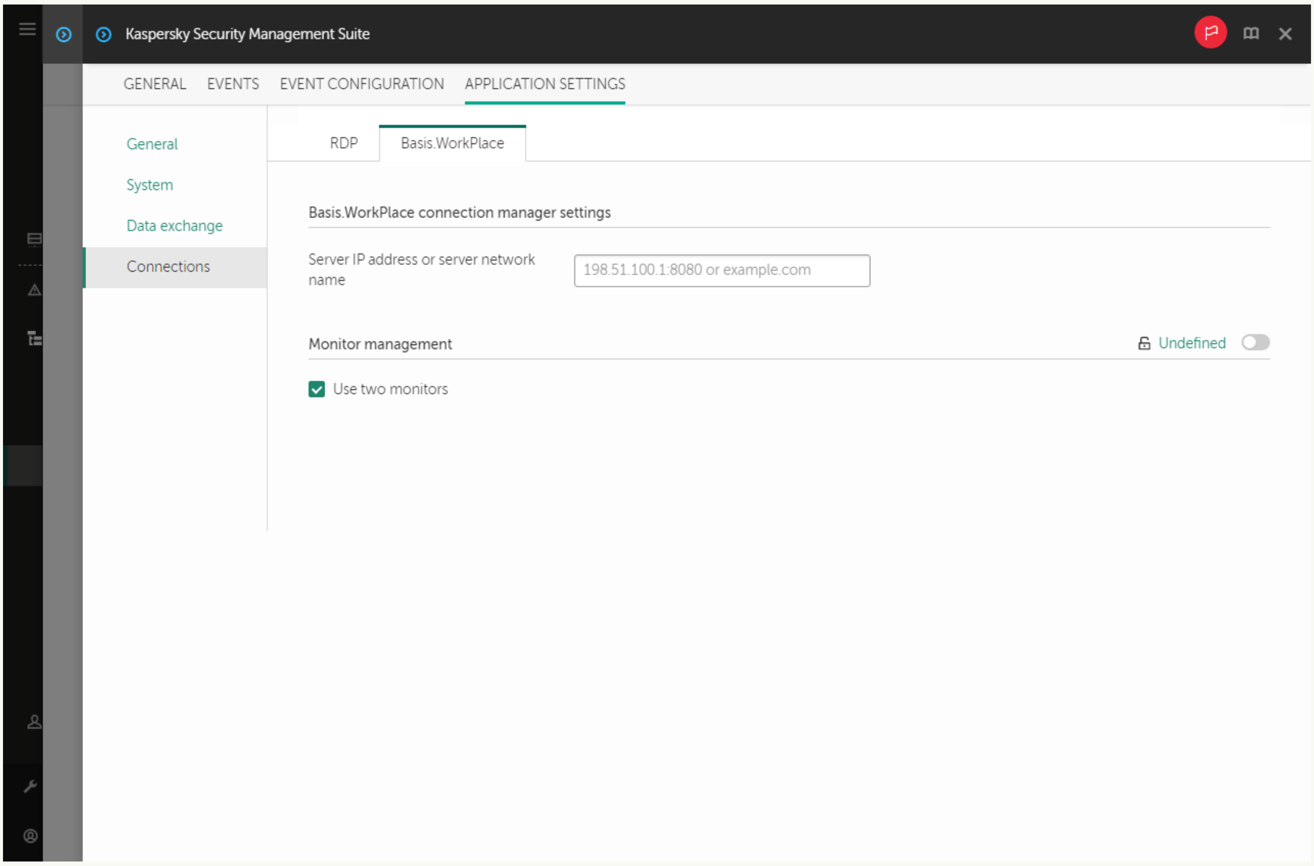
4. Click the name of the Kaspersky Security Management Suite web plug-in.

   This opens a window containing information about Kaspersky Thin Client.

5. Select the **Application settings** tab.

6. Select **Connections** → **Basis.WorkPlace**.

   This opens a window in which you can configure settings for connecting to a remote desktop managed by Basis.WorkPlace (see the figure below).



Basis.WorkPlace connection manager settings

Server IP address or server network name: 198.51.100.1:8080 or example.com

Monitor management — Undefined

☑ Use two monitors

Window for configuring settings for connecting to a remote desktop managed by Basis.WorkPlace through the Web Console for one device

7. In the **Server IP address or server network name** field, enter the IP address or server name for connecting to a remote desktop managed by Basis.WorkPlace.

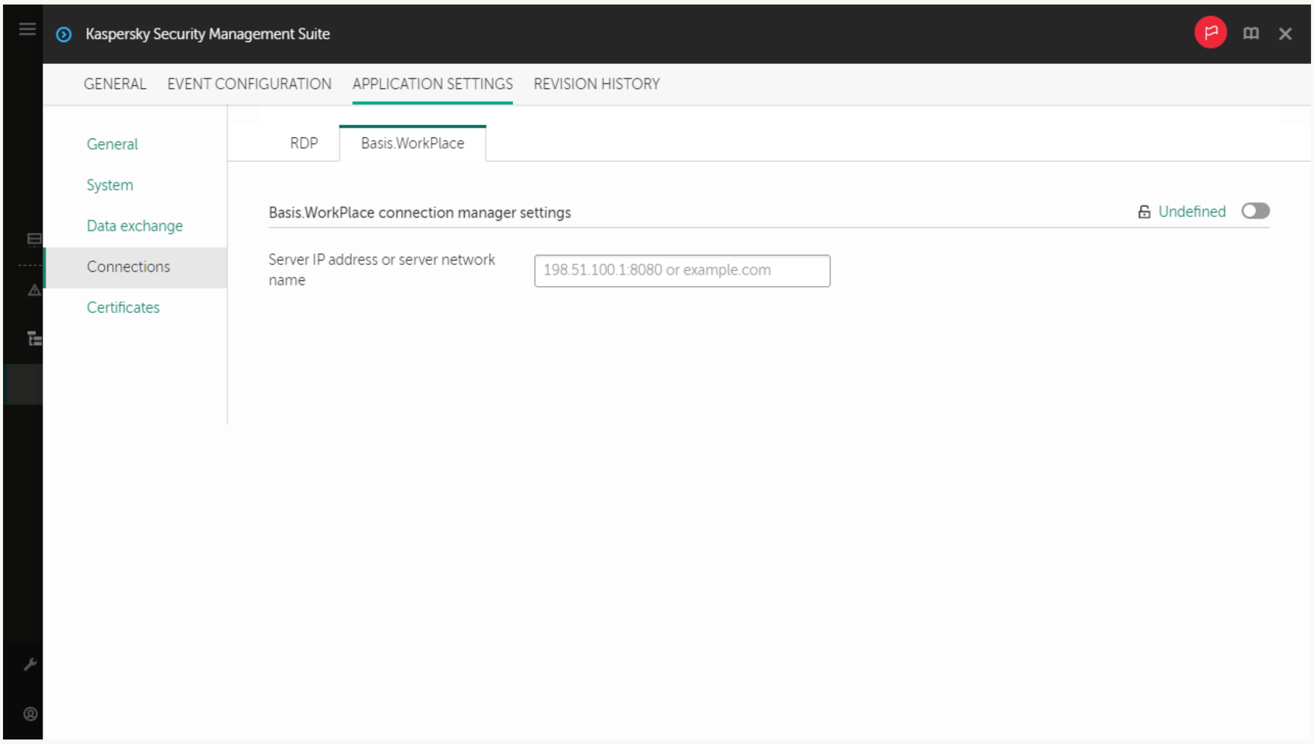
8. If two monitors are installed at your workstation and you want a remote desktop image to be displayed on both monitors, select the **Use two monitors** check box in the **Monitor management** block.

9. Click **Save** in the lower part of the window to save the changes.

How to configure settings for connecting to a remote desktop managed by Basis.WorkPlace for a group of devices

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name for the Kaspersky Security Management Suite web plug-in.
3. In the window that opens, select the **Application settings** tab.
4. Select **Connections** → **Basis.WorkPlace**.

   This opens a window in which you can configure settings for connecting to a remote desktop managed by Basis.WorkPlace (see the figure below).



Basis.WorkPlace connection manager settings — Undefined

Server IP address or server network name: 198.51.100.1:8080 or example.com

Window for configuring settings for connecting to a remote desktop managed by Basis.WorkPlace through the Web Console for a group of devices

5. In the **Server IP address or server network name** field, enter the IP address or server name for connecting to a remote desktop managed by Basis.WorkPlace.
6. Click **Save** in the lower part of the window to save the changes.

If the toggle button next to the name of a group of settings is in the **Enforced** position (Enforced ●), the defined values of these settings are applied to devices on which the policy is applied, and these settings cannot be changed in the Kaspersky Thin Client interface. If the toggle button next to the name of a group of settings is in the **Undefined** position (Undefined ○), the defined values of these settings are not applied to devices on which the policy is applied, and these settings can be changed for managed devices in the Kaspersky Thin Client interface under **Devices** → **Managed devices**.

Managing Kaspersky Thin Client power-saving mode through the Web Console

In the Web Console, you can configure power-saving mode for one device or for a group of devices running Kaspersky Thin Client.

How to configure power-saving mode for one device ?

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device where Kaspersky Thin Client is running. You can view the device name in the control panel of the Kaspersky Thin Client interface. If the computer name is not on the list, add it to the Managed devices group. You can also manage devices that have not yet been added to the managed devices group by selecting **Discovery & deployment** → **Unassigned devices**.

   > If a managed device is added to an administration group and an enforced policy is configured for the settings of this group, the settings that were individually configured for this device will not be applied.

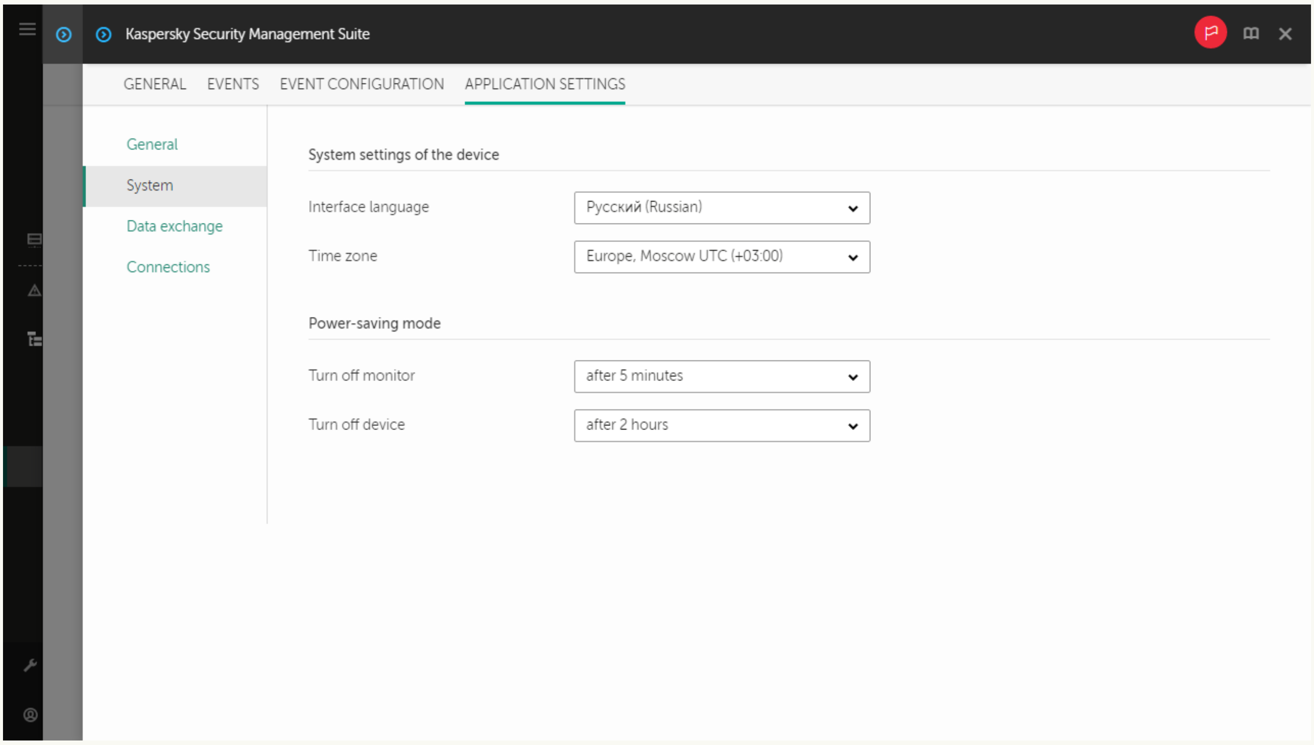
3. In the window that opens, select the **Applications** tab.

4. Click the name of the Kaspersky Security Management Suite web plug-in.

   This opens a window containing information about Kaspersky Thin Client.

5. Select the **Application settings** tab.

6. Select the **System** section (see the figure below).



System settings of the device

Interface language: Русский (Russian)

Time zone: Europe, Moscow UTC (+03:00)

Power-saving mode

Turn off monitor: after 5 minutes

Turn off device: after 2 hours

Window for configuring power-saving mode through the Web Console for one device

7. In the **Power-saving mode** block, configure the following settings:

   - In the **Turn off monitor** drop-down list, select the system inactivity period after which the monitor will be switched to power-saving mode.

   - In the **Turn off device** drop-down list, select the system inactivity period after which the thin client will be turned off.

8. Click **Save** in the lower part of the window to save the changes.

After Kaspersky Thin Client is synchronized with Kaspersky Security Center, the power-saving mode settings will be applied to Kaspersky Thin Client.

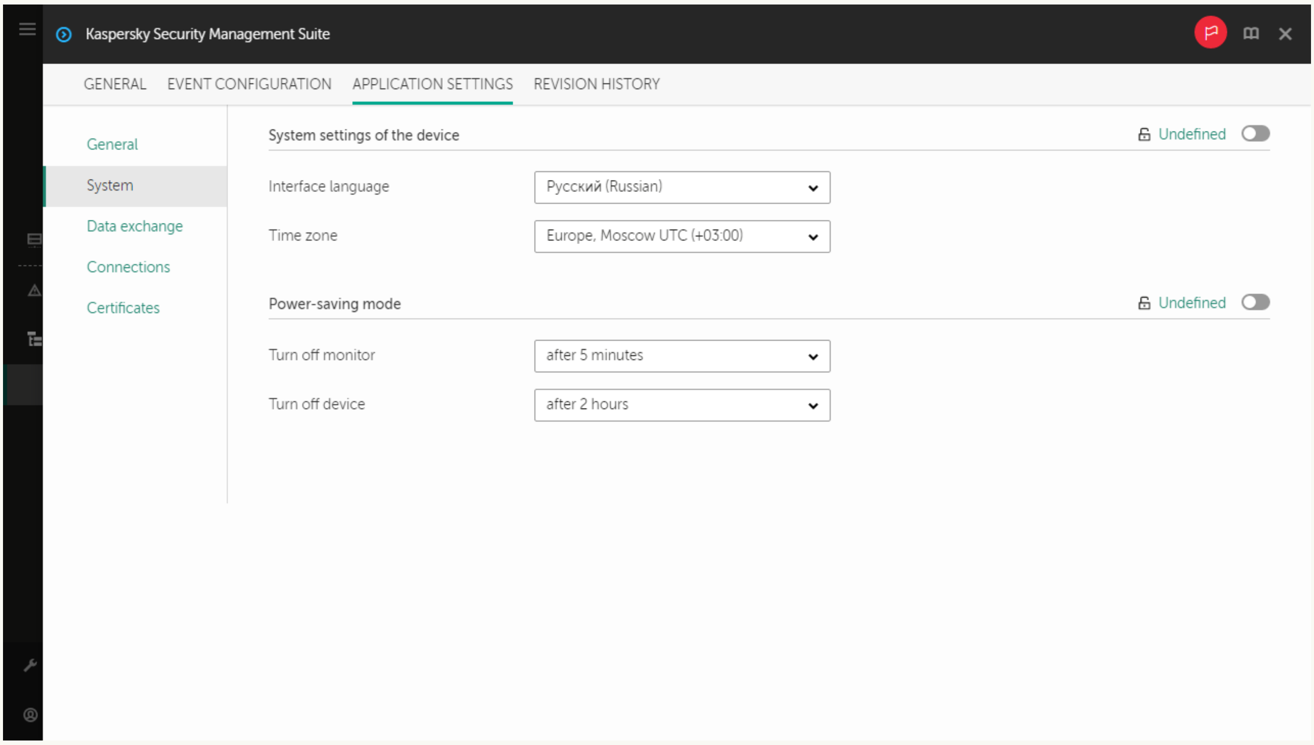
How to configure power-saving mode for a group of devices ?

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name for the Kaspersky Security Management Suite web plug-in.

3. In the window that opens, select the **Application settings** tab.

4. Select the **System** section (see the figure below).



System settings of the device — Undefined

Interface language: Русский (Russian)

Time zone: Europe, Moscow UTC (+03:00)

Power-saving mode — Undefined

Turn off monitor: after 5 minutes

Turn off device: after 2 hours

Window for configuring power-saving mode through the Web Console for a group of devices

5. In the **Power-saving mode** block, configure the following settings:

   - In the **Turn off monitor** drop-down list, select the system inactivity period after which the monitor will be switched to power-saving mode.

   - In the **Turn off device** drop-down list, select the system inactivity period after which the thin client will be turned off.

6. Click **Save** in the lower part of the window to save the changes.

After all devices of an administration group are synchronized with Kaspersky Security Center, the power-saving mode settings will be applied to all Kaspersky Thin Clients included in this group.

If the toggle button next to the name of a group of settings is in the **Enforced** position (🔒 Enforced ●), the defined values of these settings are applied to devices on which the policy is applied, and these settings cannot be changed in the Kaspersky Thin Client interface. If the toggle button next to the name of a group of settings is in the **Undefined** position (🔒 Undefined ○), the defined values of these settings are not applied to devices on which the policy is applied, and these settings can be changed for managed devices in the Kaspersky Thin Client interface under **Devices** → **Managed devices**.

Configuring the interface language and time zone of Kaspersky Thin Client through the Web Console

In the Web Console, you can configure the interface language and time zone for one device or for a group of devices running Kaspersky Thin Client.

How to configure the interface language and time zone for one device ?

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device where Kaspersky Thin Client is running. You can view the device name in the control panel of the Kaspersky Thin Client interface. If the computer name is not on the list, add it to the Managed devices group. You can also manage devices that have not yet been added to the managed devices group by selecting **Discovery & deployment** → **Unassigned devices**.

   > If a managed device is added to an administration group and an enforced policy is configured for the settings of this group, the settings that were individually configured for this device will not be applied.

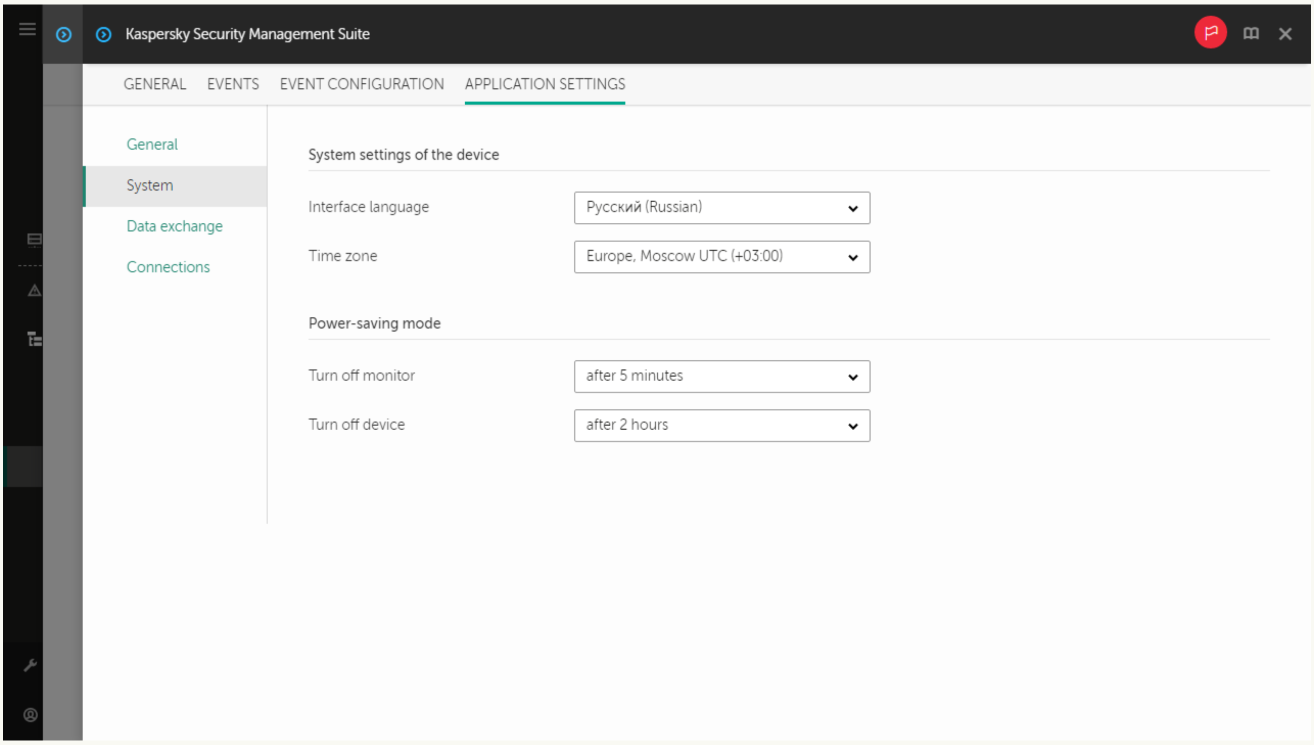
3. In the window that opens, select the **Applications** tab.

4. Click the name of the Kaspersky Security Management Suite web plug-in.

   This opens a window containing information about Kaspersky Thin Client.

5. Select the **Application settings** tab.

6. Select the **System** section (see the figure below).



System settings of the device

Interface language: Русский (Russian)

Time zone: Europe, Moscow UTC (+03:00)

Power-saving mode

Turn off monitor: after 5 minutes

Turn off device: after 2 hours

Window for configuring the interface language and time zone through the Web Console for one device

7. In the **System settings of the device** block, select the relevant values from the **Interface language** and **Time zone** drop-down lists.

8. Click **Save** in the lower part of the window to save the changes.

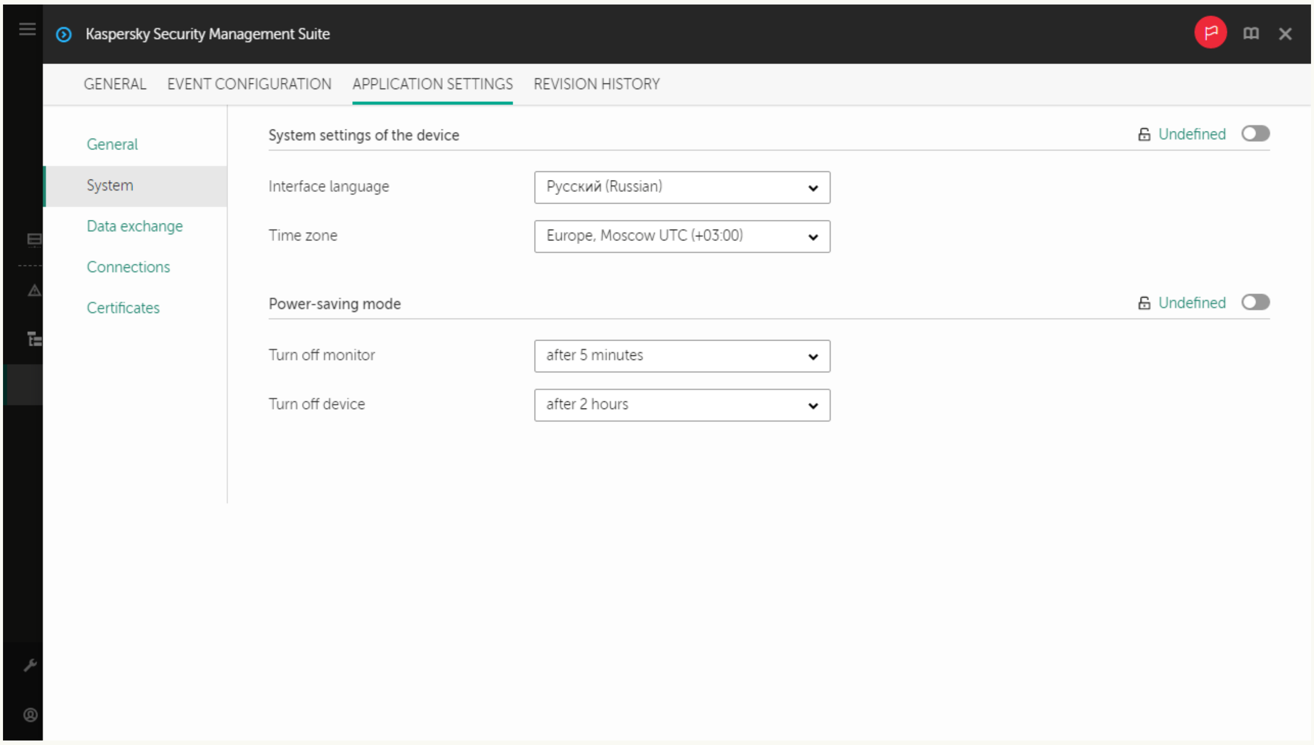
How to configure the interface language and time zone for a group of devices

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name for the Kaspersky Security Management Suite web plug-in.

3. In the window that opens, select the **Application settings** tab.

4. Select the **System** section (see the figure below).



System settings of the device — Undefined

Interface language: Русский (Russian)

Time zone: Europe, Moscow UTC (+03:00)

Power-saving mode — Undefined

Turn off monitor: after 5 minutes

Turn off device: after 2 hours

Window for configuring the interface language and time zone through the Web Console for a group of devices

5. In the **System settings of the device** block, select the relevant values from the **Interface language** and **Time zone** drop-down lists.

6. Click **Save** in the lower part of the window to save the changes.

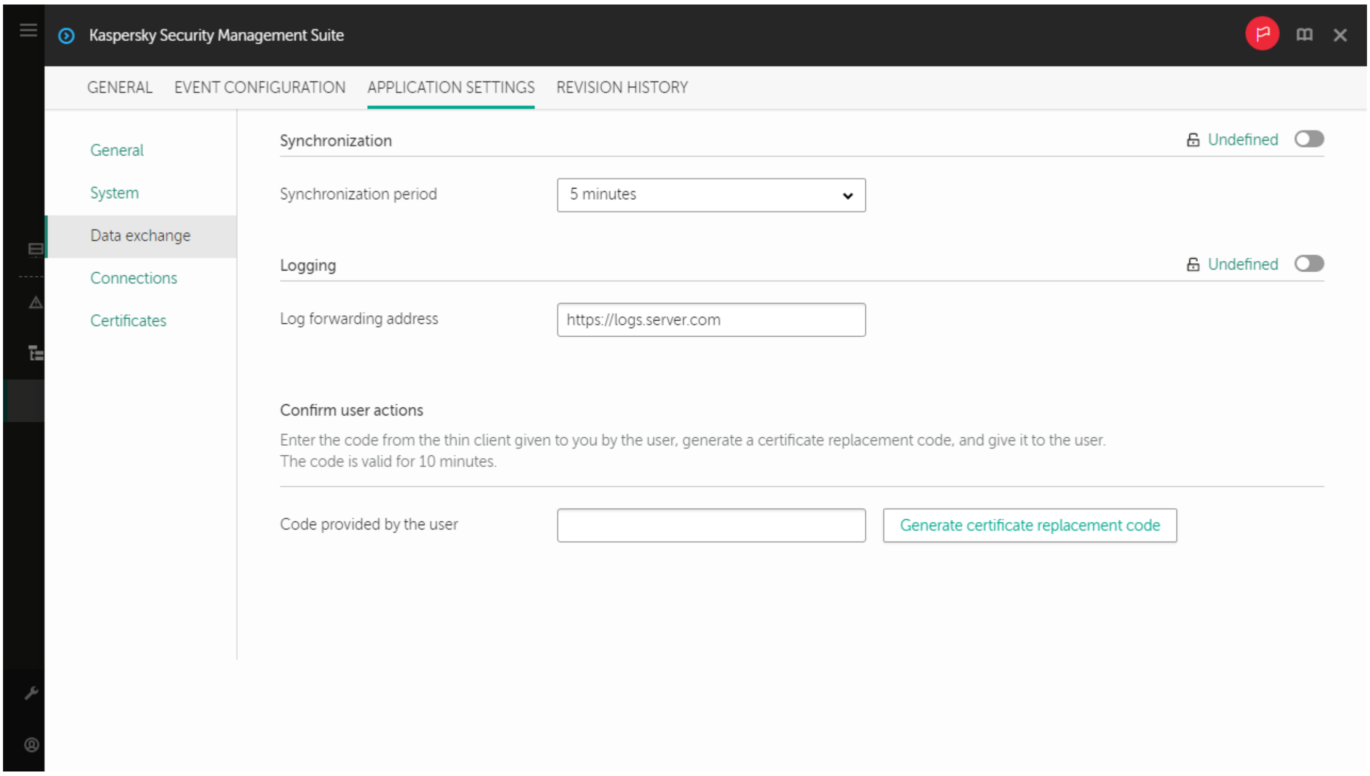
If the toggle button next to the name of a group of settings is in the **Enforced** position (Enforced ●), the defined values of these settings are applied to devices on which the policy is applied, and these settings cannot be changed in the Kaspersky Thin Client interface. If the toggle button next to the name of a group of settings is in the **Undefined** position (Undefined ○), the defined values of these settings are not applied to devices on which the policy is applied, and these settings can be changed for managed devices in the Kaspersky Thin Client interface under **Devices** → **Managed devices**.

Configuring synchronization between Kaspersky Thin Client and Kaspersky Security Center

In the Web Console, you can configure synchronization with Kaspersky Security Center only for a group of devices running Kaspersky Thin Client.

To configure synchronization between Kaspersky Thin Client and Kaspersky Security Center:

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name for the Kaspersky Security Management Suite web plug-in.
3. In the window that opens, select the **Application settings** tab.
4. Select the **Data exchange** section (see the figure below).



Kaspersky Security Management Suite

GENERAL | EVENT CONFIGURATION | APPLICATION SETTINGS | REVISION HISTORY

General
System
Data exchange
Connections
Certificates

Synchronization — Undefined

Synchronization period: 5 minutes

Logging — Undefined

Log forwarding address: https://logs.server.com

Confirm user actions

Enter the code from the thin client given to you by the user, generate a certificate replacement code, and give it to the user.
The code is valid for 10 minutes.

Code provided by the user

Generate certificate replacement code

Window for configuring synchronization between Kaspersky Thin Client and Kaspersky Security Center

5. In the **Synchronization period** field, specify the interval for synchronizing Kaspersky Thin Client with Kaspersky Security Center.
6. Click **Save** in the lower part of the window to save the changes.

If the toggle button next to the name of a group of settings is in the **Enforced** position (Enforced ●), the defined values of these settings are applied to devices on which the policy is applied, and these settings cannot be changed in the Kaspersky Thin Client interface. If the toggle button next to the name of a group of settings is in the **Undefined** position (Undefined ○), the defined values of these settings are not applied to devices on which the policy is applied, and these settings can be changed for managed devices in the Kaspersky Thin Client interface under **Devices** → **Managed devices**.

Configuring forwarding of Kaspersky Thin Client logs to a log server

In the Web Console, you can configure forwarding of Kaspersky Thin Client logs to a log server for one device or for a group of devices running Kaspersky Thin Client.

How to configure forwarding of logs for one device

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device where Kaspersky Thin Client is running. You can view the device name in the control panel of the Kaspersky Thin Client interface. If the computer name is not on the list, add it to the Managed devices group. You can also manage devices that have not yet been added to the managed devices group by selecting **Discovery & deployment** → **Unassigned devices**.

   > If a managed device is added to an administration group and an enforced policy is configured for the settings of this group, the settings that were individually configured for this device will not be applied.

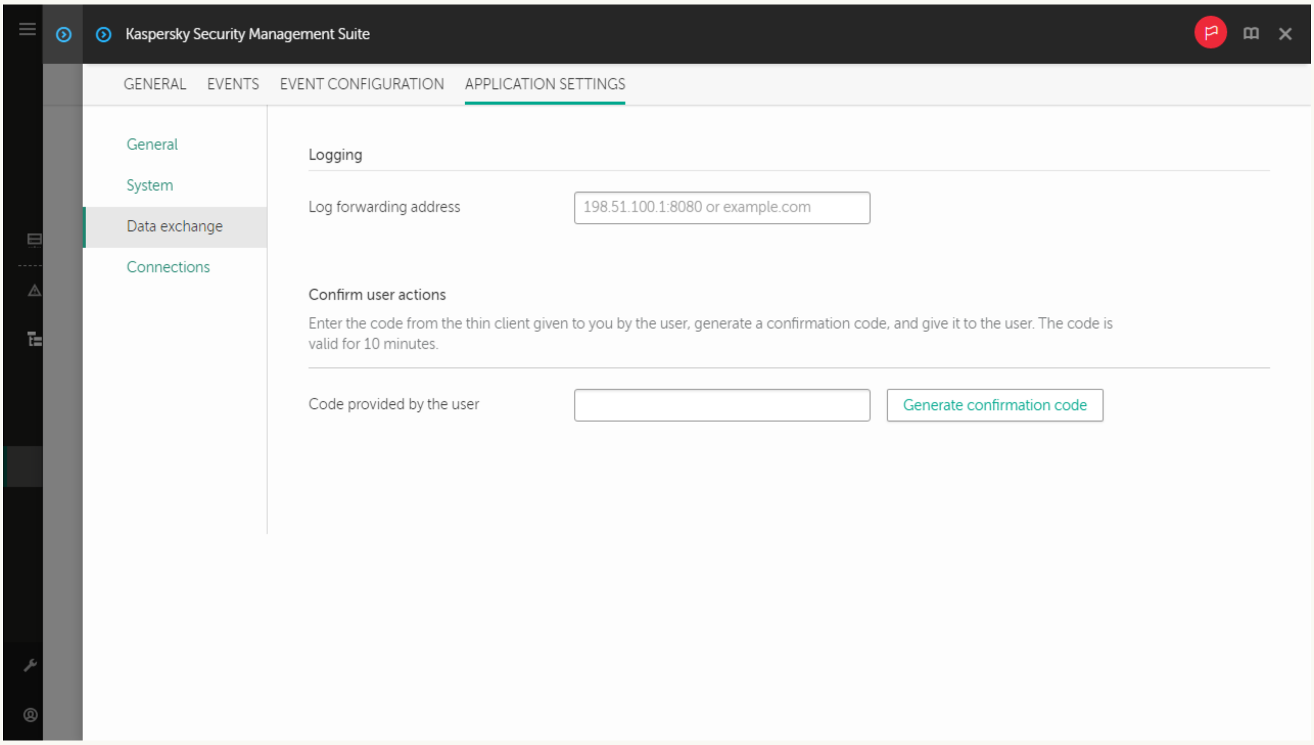
3. In the window that opens, select the **Applications** tab.

4. Click the name of the Kaspersky Security Management Suite web plug-in.

   This opens a window containing information about Kaspersky Thin Client.

5. Select the **Application settings** tab.

6. Select the **Data exchange** section (see the figure below).



Logging

Log forwarding address: 198.51.100.1:8080 or example.com

Confirm user actions

Enter the code from the thin client given to you by the user, generate a confirmation code, and give it to the user. The code is valid for 10 minutes.

Code provided by the user:

Window for configuring forwarding of Kaspersky Thin Client logs through the Web Console for one device

7. In the **Log forwarding address** field, enter the address of the destination log server in the format https://<server address>. Make sure that a log server compliant with the requirements is deployed in the enterprise infrastructure.

8. Click **Save** in the lower part of the window to save the changes.

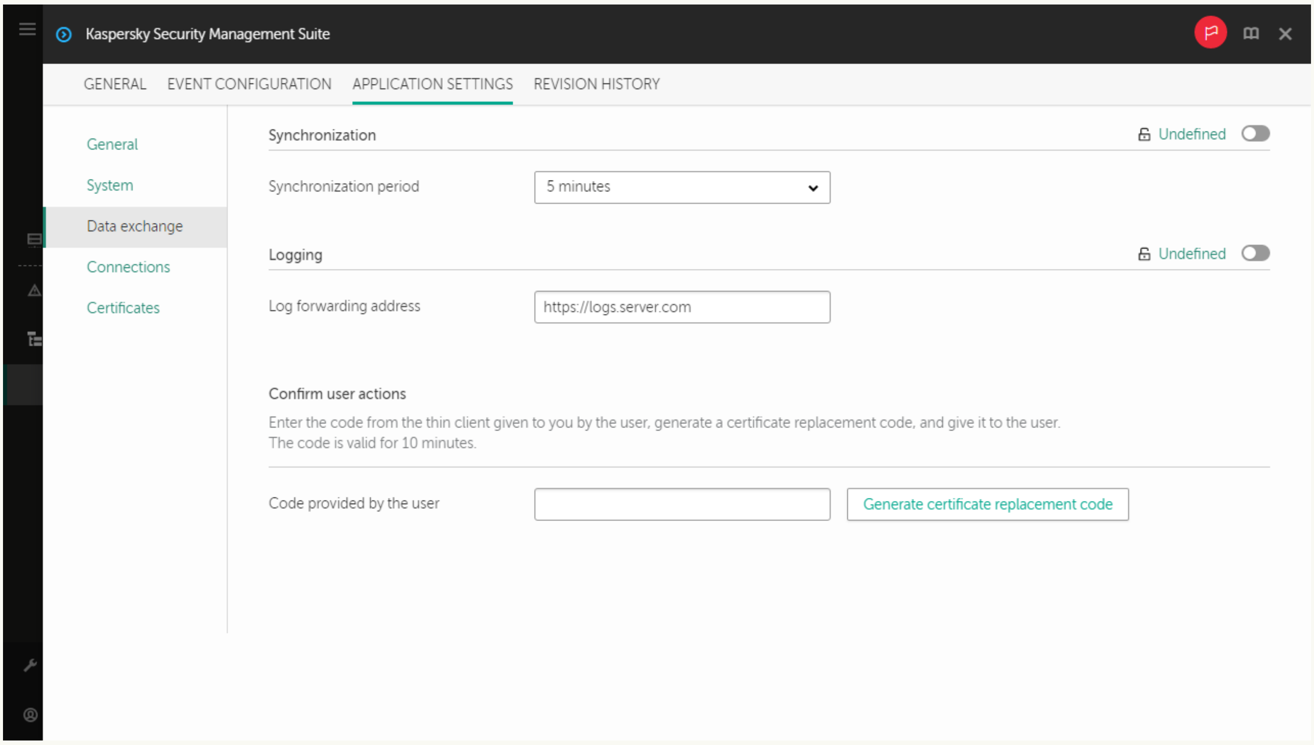
How to configure forwarding of logs for a group of devices

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name for the Kaspersky Security Management Suite web plug-in.

3. In the window that opens, select the **Application settings** tab.

4. Select the **Data exchange** section (see the figure below).



Synchronization period: 5 minutes

Log forwarding address: https://logs.server.com

Confirm user actions

Enter the code from the thin client given to you by the user, generate a certificate replacement code, and give it to the user.
The code is valid for 10 minutes.

Code provided by the user

Window for configuring forwarding of Kaspersky Thin Client logs through the Web Console for a group of devices

5. In the **Log forwarding address** field, enter the address of the destination log server in the format https://<server address>. Make sure that a log server compliant with the requirements is deployed in the enterprise infrastructure.

6. Click **Save** in the lower part of the window to save the changes.

Confirming Kaspersky Thin Client user actions

The following user actions require confirmation from the Kaspersky Security Center administrator:

- changing settings for connecting to Kaspersky Security Center
- changing certificates for connecting to Kaspersky Security Center
- resetting all settings and data of a thin client

To confirm the change of settings for connecting to Kaspersky Security Center or reset of all thin client settings:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device where Kaspersky Thin Client is running. You can view the device name in the control panel of the Kaspersky Thin Client interface. If the computer name is not on the list, add it to the Managed devices group. You can also manage devices that have not yet been added to the managed devices group by selecting **Discovery & deployment** → **Unassigned devices**.

> If a managed device is added to an administration group and an enforced policy is configured for the settings of this group, the settings that were individually configured for this device will not be applied.

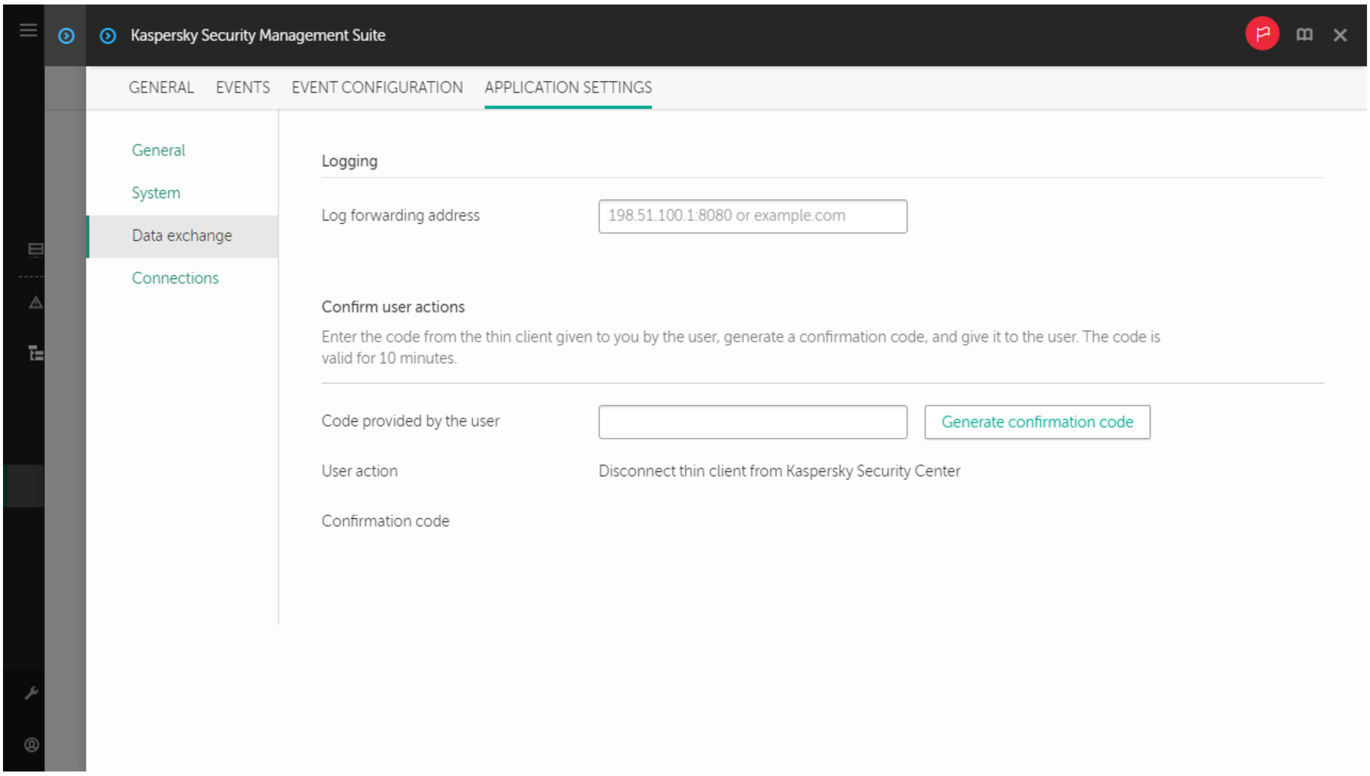
3. In the window that opens, select the **Applications** tab.

4. Click the name of the Kaspersky Security Management Suite web plug-in.

   This opens a window containing information about Kaspersky Thin Client.

5. Select the **Application settings** tab.

6. Select the **Data exchange** section (see the figure below).



Logging

Log forwarding address: 198.51.100.1:8080 or example.com

Confirm user actions

Enter the code from the thin client given to you by the user, generate a confirmation code, and give it to the user. The code is valid for 10 minutes.

Code provided by the user

User action: Disconnect thin client from Kaspersky Security Center

Confirmation code

Window for confirming changes to Kaspersky Security Center connection settings

7. In the **Confirm user actions** block, enter the code from the Kaspersky Thin Client interface which the user sent you and click **Generate confirmation code**.

   A confirmation code will be created and displayed in the **Confirm user actions** block.

8. Send the confirmation code to the Kaspersky Thin Client user.

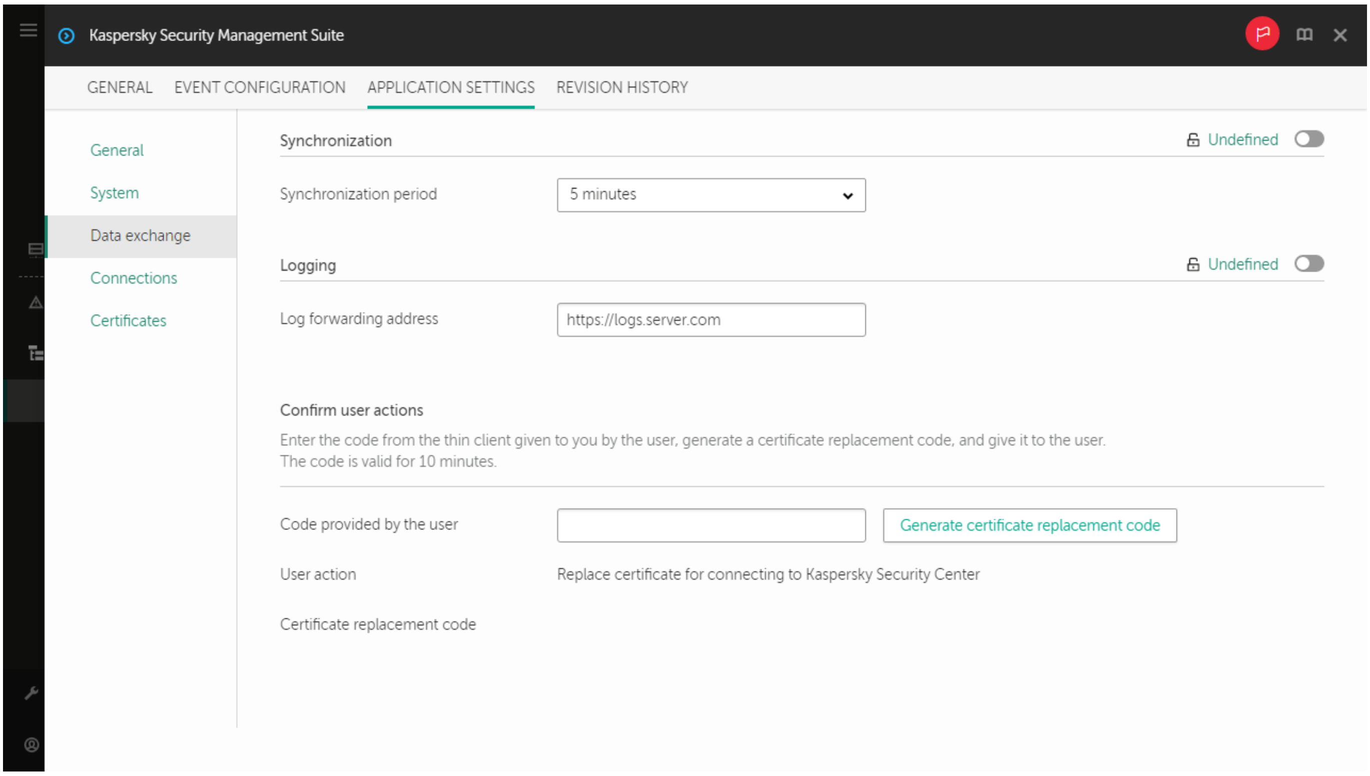
To confirm the change of the certificate for connecting to Kaspersky Security Center:

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name for the Kaspersky Security Management Suite web plug-in.

3. In the window that opens, select the **Application settings** tab.

4. Select the **Data exchange** section (see the figure below).



Synchronization — Undefined

Synchronization period: 5 minutes

Logging — Undefined

Log forwarding address: https://logs.server.com

Confirm user actions

Enter the code from the thin client given to you by the user, generate a certificate replacement code, and give it to the user.
The code is valid for 10 minutes.

Code provided by the user

Generate certificate replacement code

User action: Replace certificate for connecting to Kaspersky Security Center

Certificate replacement code

Window for confirming changes to the certificate for connecting to Kaspersky Security Center

5. In the **Confirm user actions** block, enter the code from the Kaspersky Thin Client interface which the user sent you and click **Generate certificate replacement code**.

   A certificate replacement code will be created and displayed in the **Confirm user actions** block.

6. Send the certificate replacement code to the Kaspersky Thin Client user.

Managing Kaspersky Thin Client security certificates through the Web Console

You can use the Web Console to manage security certificates for a group of devices that have the Kaspersky Thin Client operating system installed. You can view valid certificates, add certificates, or delete them.

> After security certificates for connecting to remote desktops or to a log server are added in the Kaspersky Security Center Web Console, thin clients in the administration group will switch to trusted mode. In this case, you will not be able to add certificates through the Kaspersky Thin Client interface.

In the **Certificates** section, the following information is displayed for each valid certificate:

- **File name** shows a certificate file name and its format.
- **Issuer name** shows information about the organization that issued the certificate.
- **Subject name** shows information about the application for which the certificate was issued.
- **Valid from** shows a start date of certificate validity.

- **Valid to** shows an end date of certificate validity.
- **Certificate fingerprint** shows certificate hash calculated from all certificate details and its signature.

You can sort the list of certificates based on their validity start and end dates, issuer and subject names.

About the reserve certificate for connecting Kaspersky Thin Client to Kaspersky Security Center

To connect to Kaspersky Security Center, Kaspersky Thin Client uses a mobile certificate of the Kaspersky Security Center Administration Server. This mobile certificate is created by using the *Administration Server quick start wizard* after installing Kaspersky Security Center. The default validity period of an issued certificate is one year. When connecting to Kaspersky Security Center, Kaspersky Thin Client checks the validity of the certificate. If necessary, you can issue a new (reserve) mobile certificate or configure a rule for issuing certificates. For details on creating a new mobile certificate for the Kaspersky Security Center Administration Server, see the *Working with certificates of mobile devices* section and the *Reissuing the Web Server certificate* section of the Kaspersky Security Center Online Help Guide. For details on configuring rules for issuing certificates, see the *Configuring certificate issuance rules* section of the Kaspersky Security Center Online Help Guide.

Managed devices and devices included in an administration group will receive the new (reserve) certificate for connecting Kaspersky Thin Client to Kaspersky Security Center after Kaspersky Thin Client synchronizes with Kaspersky Security Center. The new (reserve) certificate will be saved in the Kaspersky Thin Client certificate store and will be used to connect thin clients to Kaspersky Security Center when the currently used certificate expires.

You can also issue a user certificate for connecting Kaspersky Thin Client to Kaspersky Security Center. In this case, the created user certificate must be uploaded to the Web Console as the mobile certificate. For detailed information about the requirements applied to Kaspersky Security Center user certificates, see the *Requirements for custom certificates used in Kaspersky Security Center* section in the Kaspersky Security Center Online Help Guide.

Creating a user certificate for connecting Kaspersky Thin Client to Kaspersky Security Center

You can use a user certificate for connecting Kaspersky Thin Client to Kaspersky Security Center. For detailed information about the requirements applied to Kaspersky Security Center certificates, see the *Requirements for custom certificates used in Kaspersky Security Center* section of the Kaspersky Security Center Online Help Guide. We recommend using a user certificate when migrating a group of devices running Kaspersky Thin Client to a new Kaspersky Security Center Administration Server. After the user certificate is created, it must be uploaded to the Web Console as a mobile certificate. You can use the OpenSSL tool to create a user certificate.

To create a user certificate for connecting Kaspersky Thin Client to Kaspersky Security Center using the OpenSSL tool:

1. Start the console and go to the folder in which you want to create the certificate.
2. In the console, start the OpenSSL tool and run the following command:

   ```
   openssl req -x509 -newkey rsa:2048 -keyout key.pem -out server.pem -days 729 -subj
   '/CN=mydomain.ru/C=RU/L=Moscow/O=My Organization Name/OU=My Organization Unit Name' -
   addext "keyUsage = digitalSignature, keyEncipherment, dataEncipherment, cRLSign,
   keyCertSign" -addext "extendedKeyUsage = serverAuth, clientAuth"
   ```

   where:

  - `-keyout key.pem` is a name of the file in which the private key of the created certificate will be saved.
  - `-out server.pem` is a name of the file in which the created certificate will be saved.
  - `-days` is a setting that defines the validity term of the created certificate, in days. We recommend setting a certificate validity term of no more than 729 days.
  - `-subj '/CN=mydomain.ru/C=RU/L=Moscow/O=My Organization Name/OU=My Organization Unit Name'` is data of your organization: domain name, location, name.

3. Enter and confirm the password for the private certificate key. This password will need to be entered when uploading the user certificate to the Web Console as a mobile certificate. There are no special password requirements.

   As a result, the following two files will be created in the folder where you ran the command:

- server.pem is a certificate file for connecting Kaspersky Thin Client to Kaspersky Security Center.
- key.pem is a private key of the certificate for connecting Kaspersky Thin Client to Kaspersky Security Center.

If necessary, you can convert a certificate file from PEM to DER format.

Uploading a reserve certificate and user certificate to the Web Console for connecting Kaspersky Thin Client to Kaspersky Security Center

If you created a user certificate or a reserve certificate for connecting Kaspersky Thin Client to Kaspersky Security Center, you must upload the created certificate to the Web Console as a mobile certificate.

It is recommended to first verify that the user certificate meets the requirements of Kaspersky Security Center. For detailed information about the requirements applied to Kaspersky Security Center certificates, see the *Requirements for custom certificates used in Kaspersky Security Center* section of the Kaspersky Security Center Online Help Guide.

To upload a certificate to the Web Console for connecting Kaspersky Thin Client to Kaspersky Security Center:

1. In the menu of the Kaspersky Security Center Web Console, click the 🔧 icon next to the name of the Kaspersky Security Center Administration Server.

   The **Administration Server properties** window opens.

2. In the list of subsections, select **Certificates**.

3. In the window that opens, in the **Administration Server authentication by mobile devices** block, select **Other certificate** and click the **Manage certificate** button.

4. In the panel that opens on the right, click **Browse** and do the following:

   a. In the **Certificate type** drop-down list, select **X.509 certificate**.

   b. If the user certificate is protected with a password, enter the password.

   c. Select the user certificate file by clicking the **Browse** button in the **Certificate** block.

   d. Select the private key for the user certificate by clicking the **Browse** button in the **Private key** block.

5. Click **Save** to save the certificate adding.

6. Click **Save** to save the changes you made in the **Certificates** subsection.

   The certificate for connecting Kaspersky Thin Client to Kaspersky Security Center will be uploaded to the Web Console as a mobile certificate.

Adding new certificates in the Web Console

For thin clients that are members of an administration group, you can add new certificates in the Web Console for securely connecting to remote desktops (via RDP or under Basis.WorkPlace management) or to a log server.

> After certificates for securely connecting to remote desktops or to a log server are added to the Web Console, devices in the administration group will switch to trusted mode. In this case, you will not be able to add certificates through the Kaspersky Thin Client interface.

To add new certificates through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.

2. Click the policy name for the Kaspersky Security Management Suite web plug-in.

3. In the window that opens, select the **Application settings** tab.

4. Select the **Certificates** section.

5. In the **Valid certificates** table, click the **Add** button in the upper part of the table.

6. In the panel that opens on the right, select all certificates that were previously uploaded and select the new certificates. The total size of the uploaded files must not exceed 1 MB. You can upload certificates only in DER format. Each certificate file must contain only one certificate. If necessary, you can convert certificates from PEM to DER format in advance.

7. Click **OK** to confirm the upload of the selected certificates.

   The selected certificates will be uploaded and information about them will be displayed in the **Valid certificates** table.

Removing certificates from the Web Console

For thin clients that are members of an administration group, you can remove the certificates for securely connecting to remote desktops (via RDP or under Basis.WorkPlace management) or to a log server from the Web Console.

> When you remove a certificate, you will no longer be able to use the Kaspersky Thin Client interface to securely connect to servers where this certificate or its signed certificates are installed.

After certificates for securely connecting to remote desktops or to a log server are removed from the Web Console, Kaspersky Thin Client devices that are members an administration group will be switched out of the trusted mode. To connect to remote desktops or to a log server, you will have to add certificates in the Kaspersky Thin Client interface.

To remove certificates:

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name for the Kaspersky Security Management Suite web plug-in.
3. In the window that opens, select the **Application settings** tab.
4. Select the **Certificates** section.
5. In the **Valid certificates** table, select the check boxes next to the certificates that you need to remove.
6. Click **Delete** and confirm deletion.

The selected certificates will be removed.

Converting a certificate from PEM to DER format

Kaspersky Security Management Suite supports uploading of certificates only in DER format. You can convert a certificate file from PEM to DER format.

To carry out these instructions on the local computer, you must have the OpenSSL tool.

To convert a certificate file from PEM to DER format:

1. Start the console on the local computer.
2. Go to the folder containing the PEM certificate file and run the following file conversion command:

```
openssl x509 -outform der -in <certificate file name>.pem -out <certificate file name>.der
```

where:

- <certificate file name>.pem is the original certificate file name in PEM format.
- <certificate file name>.der is the converted certificate file name in DER format.

The new certificate file in DER format will be generated in this same folder.

Monitoring Kaspersky Thin Client events through the Kaspersky Security Center Web Console

This section contains instructions on monitoring events registered in Kaspersky Thin Client through the Kaspersky Security Center Web Console.

Configuring registration of Kaspersky Thin Client event notifications in the Kaspersky Security Center Web Console

Kaspersky Security Center lets you receive information about events that occur while Kaspersky Thin Client is running. In the Kaspersky Security Center Web Console interface, you can configure a notification regarding the registration of such events. Each event in Kaspersky Security Center has its own severity level. Depending on the conditions of its occurrence, an event can be assigned one of the following severity levels:

- 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 requires attention because it emphasizes important situations in the operation of Kaspersky Thin Client and may indicate a possible issue 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* is an event that informs about successful completion of an operation, proper functioning of the application, or completion of a procedure.

You can configure notifications about Kaspersky Thin Client events in the Kaspersky Security Center Web Console for one device or for a group of devices.

How to configure event notifications for one device ?

1. Select **Devices** → **Managed devices** in the main window of the Kaspersky Security Center Web Console.

2. Click the name of the device where Kaspersky Thin Client is running. You can view the device name in the control panel of the Kaspersky Thin Client interface. If the computer name is not on the list, add it to the Managed devices group.

3. In the window that opens, select the **Applications** tab.

4. Click the name of the Kaspersky Security Management Suite web plug-in.

   This opens a window containing information about Kaspersky Thin Client.

5. Select the **Event configuration** tab.

6. Select the severity of events whose information you want to receive:

   - **Critical**
   - **Functional failure**
   - **Warning**
   - **Info**

   A table of events for the selected severity level will be displayed.

7. Click the **Add event** button and in the window that opens select the check box next to the types of events that you want to add.

8. Click **OK**.

9. To save the changes, click the **Save** button.

Kaspersky Thin Client will send the selected types of events with the specified severity to the Kaspersky Security Center Administration Server. The default storage time for events is 30 days.

How to configure event notifications for a group of devices

1. In the main window of the Web Console, select **Devices** → **Policies & profiles**.
2. Click the policy name for the Kaspersky Security Management Suite web plug-in.
3. In the window that opens, select the **Event configuration** tab.
4. Select the severity of events whose information you want to receive:
   - **Critical**
   - **Functional failure**
   - **Warning**
   - **Info**

   A table of events for the selected severity level will be displayed.
5. Click the **Add event** button and in the window that opens select the check box next to the types of events that you want to add.
6. Click **OK**.
7. To save the changes, click the **Save** button.

If the **Enforced** toggle button is turned off, the settings will not be applied to Kaspersky Thin Client devices that are in the administration group and are covered by the current security policy.

Kaspersky Thin Client will send the selected types of events with the specified severity to the Kaspersky Security Center Administration Server. The default storage time for events is 30 days.

For detailed information on configuring notifications for event registration in the Kaspersky Security Center Web Console, please refer to the *Configuring notification delivery* section of the Kaspersky Security Center Online Help Guide.

Viewing Kaspersky Thin Client events in the Web Console

You can view events registered by Kaspersky Thin Client in the Web Console.

To view events registered by Kaspersky Thin Client in the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the thin client where Kaspersky Thin Client is running.
3. In the window that opens, select the **Events** tab.

This opens a window displaying a table of registered events. The following information is displayed for each event:

- **Time** shows the date and time when the Web Console received the event registered on a device.

- **Event** shows a type of the event.
- **Description** shows a short description of the registered event.
- **Application** shows a name of the application for which the event was received in the Web Console.
- **Version number** shows a version of the application for which the event was received in the Web Console.
- **Severity level** shows severity of the event (*Critical*, *Functional failure*, *Warning* or *Info*).
- **Task** shows a name of the task to be run when the event is registered.
- **Registered** shows the date and time when the event was registered on the device.

Troubleshooting

If an error occurs, check the following:

1. The thin client is turned on.
2. The thin client is connected to the network.
3. The correct IP address or server name, user name and password were entered when connecting to the remote desktop.

If you are unable to resolve the error, please contact Technical Support. If necessary, Technical Support experts may ask you to provide system information and/or the event log.

Disconnecting from a remote desktop

If you encounter an error that causes Kaspersky Thin Client to disconnect from a remote desktop, the remote desktop screen closes and shows a message with the malfunction reason.

To resume operation on the remote desktop:

1. Close the error message.
2. Try to connect to the remote desktop.
3. If the connection fails, restart the thin client and try to connect to the remote desktop again.
4. If a connection still cannot be established, please contact your enterprise administrator to fix any physical issues that could be causing Kaspersky Thin Client to disconnect from the remote desktop.
5. If the physical connection is good but you still cannot connect to the remote desktop, please contact Technical Support.

Incorrectly entered data

Prior to initiating a remote desktop connection, Kaspersky Thin Client verifies that the following user-entered data is correct:

- IP address or server name
- user name
- password

If the format of the entered data differs from the data format expected by the system, an invalid data error is displayed in the lower part of the remote desktop connection window.

> There may be multiple errors, in which case you need to move your cursor over the message in the lower part of the remote desktop connection window to view the entire errors list in a tooltip window.

To connect to the remote desktop:

1. Enter the correct IP address or server name, user name, and password.
2. If you are sure that you correctly entered the user name and password but an error is still displayed when you try to connect, make sure that you enter the correct name or IP address of the server to which you want to connect.

Testing the network connection

To test whether the thin client is connected to the network,

View the status of Kaspersky Thin Client connections to the network and to Kaspersky Security Center ? in the Kaspersky Thin Client control panel.

Contacting Technical Support

If you experience problems that you cannot resolve on your own when working with Kaspersky Thin Client, please contact TONK Technical Support.

When you contact Technical Support, experts may ask you to provide audit and event logs of Kaspersky Thin Client. These logs are located on the device with Kaspersky Thin Client system installed. You can view the event logs in the Kaspersky Thin Client interface under **Tools** → **Event log**. You can also forward audit and event logs to a log server deployed in the infrastructure of your enterprise.

Glossary

Administration group

A set of devices combined according to the performed functions. Devices are grouped for easy management as a whole. A group may include other groups. Group policies can be created for each thin client added to a group.

Administration Server

A component of the Kaspersky Security Center application that provides centralized storage and management of information about Kaspersky applications installed in an enterprise's network.

Event

An entry containing records of changes made to the state or configuration of a thin client, or errors that require the attention of a system administrator.

Kaspersky Security Center administrator

A person who manages thin client operations through the remote centralized administration system known as Kaspersky Security Center.

Kaspersky Security Management Suite web plug-in

A specialized component that provides an interface for managing Kaspersky Thin Client settings through the Kaspersky Security Center Administration Console.

Kaspersky update servers

Kaspersky HTTP servers from which a Kaspersky application receives updates for databases and application modules.

Managed devices

Enterprise network devices that are included into an administration group.

Policy

A policy determines settings of Kaspersky Thin Client and defines access to configuration of Kaspersky Thin Client settings on devices within an administration group. You can create an unlimited number of different policies for Kaspersky Thin Clients installed on devices in each administration group, but only one policy at a time can be applied to each Kaspersky Thin Client device within an administration group.

Thin client

A compact personal computer used for connecting via a network to remote servers that provide data storage and have all necessary for an operation applications installed. A monitor, keyboard and mouse are connected to a thin client.

TLS

Secure protocol that uses encryption to transfer data in local networks and on the internet.

Update

A procedure for replacing/adding new files (Kaspersky Thin Client databases or modules) received from Kaspersky update servers.

Information about third-party code

Information about third-party code is contained in the file named LegalNotices_en.txt, which is included in the distribution kit.

You can also view information about third-party code in the Kaspersky Thin Client interface.

To view information about third-party code,

In the Kaspersky Thin Client control panel, click ⬡ and select **Tools** → **Information about third-party code** in the menu that opens.

This opens a window showing information about the use of third-party code in the current version of Kaspersky Thin Client.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft, Windows, and Windows Server are trademarks of the Microsoft group of companies.

JavaScript is the registered trademark of Oracle and/or its affiliates.