

The Kaspersky logo is displayed in a bold, lowercase, sans-serif font. It is positioned within a large, white, rounded rectangular area that is centered on a background with a green-to-teal gradient. The background has a subtle, wavy pattern.

Kaspersky Thin Client

© 2026 AO Kaspersky Lab

Contents

[Kaspersky Thin Client Help](#)

[About Kaspersky Thin Client](#)

[Distribution kit](#)

[Operation of Kaspersky Thin Client](#)

[Hardware and software requirements](#)

[Remote connection methods](#)

[Connecting using the RDP application](#)

[Connecting using the Basis.WorkPlace application](#)

[Connecting using the Web Access application](#)

[What's new](#)

[Installing and updating Kaspersky Thin Client](#)

[Installing Kaspersky Thin Client](#)

[Updating Kaspersky Thin Client](#)

[Kaspersky Thin Client interface](#)

[Kaspersky Thin Client licensing](#)

[Data provision](#)

[Turning on and starting Kaspersky Thin Client for the first time](#)

[Restarting and turning off Kaspersky Thin Client](#)

[Using certificates in Kaspersky Thin Client](#)

[Configuring Kaspersky Thin Client](#)

[Scenario: quick start for administrators](#)

[Scenario: certificate assignment for a group of thin clients](#)

[Scenario: thin client migration to a new Kaspersky Security Center Server](#)

[Configuring general settings](#)

[Configuring network settings](#)

[Managing audio playback and recording devices](#)

[Configuring settings for connecting Kaspersky Thin Client to Kaspersky Security Center](#)

[Changing settings for connecting Kaspersky Thin Client to Kaspersky Security Center](#)

[Configuring the date and time](#)

[Configuring automatic startup and display of applications](#)

[Configuring monitors and screens](#)

[Configuring power-saving settings](#)

[Configuring remote thin client management settings in the Kaspersky Thin Client interface](#)

[Changing the type of unrecognized USB devices](#)

[Resetting Kaspersky Thin Client settings](#)

[Configuring settings for connecting to a remote environment using the RDP application](#)

[Configuring settings for connecting to a remote environment using the Basis.WorkPlace application](#)

[Managing access to Kaspersky Thin Client settings](#)

Managing Kaspersky Thin Client installed on a thin client

Scenario: working in Kaspersky Thin Client on a thin client

Connection to a remote environment

Connecting to a remote environment using the RDP application

Connecting to a remote environment using the Basis.WorkPlace application

Connecting to a remote environment using the Web Access application

Managing a remote session

Using the connection panel

Locking and unlocking a remote session

Closing a remote session

Managing audio playback and recording devices in the connection panel

Managing virtual application windows

Web Access: redirecting USB devices to a remote environment

Viewing information about Kaspersky Thin Client and a thin client

Viewing network status information

Viewing Kaspersky Thin Client notifications

Managing certificates in the Kaspersky Thin Client interface

Managing Kaspersky Thin Client using hotkeys

Managing access to remote management and to the remote environment screen

Remote connection to a thin client

Managing Kaspersky Thin Client via the Kaspersky Security Center Web Console

About the Kaspersky Security Management Suite web plug-in

Installing the Kaspersky Security Management Suite web plug-in

Updating the Kaspersky Security Management Suite web plug-in

Removing the Kaspersky Security Management Suite web plug-in

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

Logging in and out of the Web Console

Managing policies and administration groups

Creating an administration group

Adding thin clients to the administration group

Policy creation

Editing a policy

Locking settings in a policy

Configuring Kaspersky Thin Client settings for one device via the Web Console

Changing a thin client ID via the Web Console: one device

Configuring a connection to a remote environment using the RDP application via the Web Console: one device

Configuring a connection to a remote environment using the Basis.WorkPlace application via the Web Console: one device

Configuring a connection to a remote environment using the Web Access application via the Web Console: one device

Configuring monitors and screens via the Web Console: one device

Configuring the Kaspersky Thin Client system settings via the Web Console: one device

Configuring forwarding of Kaspersky Thin Client logs to a log server: one device

Kaspersky Thin Client personalization: one device

Configuring settings for remote connection to a thin client via the Web Console: one device

Configuring automatic startup and display of applications: one device

Configuring Kaspersky Thin Client settings for an administration group via the Web Console

Configuring the main Kaspersky Thin Client settings via the Web Console: administration group

Configuring a connection to a remote environment using the RDP application via the Web Console: administration group

[Configuring a connection to a remote environment using the Basis.WorkPlace application via the Web Console: administration group](#)

[Configuring a connection to a remote environment using the Web Access application via the Web Console: administration group](#)

[Configuring monitors and screens via the Web Console: administration group](#)

[Configuring the Kaspersky Thin Client system settings via the Web Console: administration group](#)

[Configuring forwarding of Kaspersky Thin Client logs to a log server: administration group](#)

[Kaspersky Thin Client personalization: administration group](#)

[Configuring settings for remote connection to a thin client via the Web Console: administration group](#)

[Configuring automatic startup and display of applications: administration group](#)

[Configuring synchronization between Kaspersky Thin Client and Kaspersky Security Center](#)

[Confirming Kaspersky Thin Client user actions](#)

[Managing Kaspersky Thin Client certificates via the Web Console](#)

[About a certificate for connecting Kaspersky Thin Client to Kaspersky Security Center](#)

[Reissuing a certificate for connecting Kaspersky Thin Client to Kaspersky Security Center using the Web Console](#)

[Creating a certificate for connecting Kaspersky Thin Client to Kaspersky Security Center](#)

[Uploading a certificate for connecting Kaspersky Thin Client to Kaspersky Security Center using the Web Console](#)

[Adding new certificates in the Web Console](#)

[Removing certificates from the Web Console](#)

[Converting a certificate from PEM to DER format](#)

[Updating a certificate when migrating to a new Kaspersky Security Center Server](#)

[Monitoring Kaspersky Thin Client events via the Kaspersky Security Center Web Console](#)

[Configuring registration of Kaspersky Thin Client event notifications via the Kaspersky Security Center Web Console](#)

[Viewing Kaspersky Thin Client events in the Web Console](#)

[Troubleshooting](#)

[Reconnecting after a remote connection failure](#)

[Problems restricting access to the Kaspersky Security Management Suite web plug-in functions](#)

[Contacting Technical Support](#)

[About Kaspersky Thin Client logs](#)

[Log forwarding](#)

[Glossary](#)

[Administration group](#)

[Administration Server](#)

[Broker](#)

[Event](#)

[Kaspersky Security Center administrator](#)

[Kaspersky Security Management Suite web plug-in](#)

[Log server](#)

[Policy](#)

[Remote desktop](#)

[Remote environment](#)

[Remote session](#)

[Thin client](#)

[TLS](#)

[Virtual application](#)

[Information about third-party code](#)

[Trademark notices](#)

Kaspersky Thin Client Help

	What's new What's new in this version of Kaspersky Thin Client.		Hardware and software requirements Supported remote environments and peripheral devices.
	Installing and updating Installing Kaspersky Thin Client on a thin client. Updating the version of Kaspersky Thin Client.		Getting started Starting thin client. Initial configuration and connecting to Kaspersky Security Center. Assigning certificates.
	Connection to a remote environment Available options for connecting to a remote environment. Connecting to a remote environment. Configuring connection settings.		Centralized control via the Kaspersky Security Center Web Console Managing policies and administration groups. Configuring thin clients with Kaspersky Thin Client.
	Advanced capabilities Managing Kaspersky Thin Client certificates. Managing access to Kaspersky Thin Client settings.		Monitoring Viewing and forwarding event and audit logs to a log server. Viewing Kaspersky Thin Client events via the Kaspersky Security Center Web Console.
	Remote management Remote connection to a thin client from your device.		Reset of settings and data Resetting Kaspersky Thin Client settings and data.

About Kaspersky Thin Client

Kaspersky Thin Client version 2.3 (hereinafter also referred to as "the system") is a Cyber Immune microkernel operating system for [thin clients](#) based on KasperskyOS. Kaspersky Thin Client is designed to connect to a remote environment and provide a workspace in it, including support for peripheral devices connected to the thin client. Kaspersky Thin Client 2.3 can be installed on [Dell™ Wyse 3040](#), [Centerm F620](#), and [TONK TN1200](#) thin clients.

This document does not provide an overview of thin client hardware components, such as controls and connectors, as this information is available in the vendor documentation for the device where Kaspersky Thin Client is installed.

Core functions of Kaspersky Thin Client:

- Connect to a remote environment:
 - Connect to remote and virtual desktops running [Microsoft® Windows®](#) operating systems via the Remote Desktop Protocol (RDP), and by using the Microsoft Remote Desktop Connection Broker.
 - Connect to terminal servers running [Microsoft Windows Server®](#) operating systems via the Remote Desktop Protocol (RDP), and by using the Microsoft Remote Desktop Connection Broker.
 - Connect to remote and virtual desktops running [Linux®](#) operating systems via the Remote Desktop Protocol (RDP).
 - Connect to virtual applications, including those deployed in the Microsoft Remote Desktop Services infrastructure or running [Microsoft® Windows®](#) operating systems, via the Remote Desktop Protocol (RDP).
 - Connect to virtual desktops deployed in the [Basis.WorkPlace](#) infrastructure.
 - Connect to virtual desktops deployed in the [Citrix Workspace™](#) infrastructure.
- Transmit remote environment screen images to monitors connected to a thin client.
- Redirect the following [devices connected to the thin client](#) to a remote environment:
 - wired and wireless keyboards and mice;
 - USB drives;
 - audio playback and recording devices (USB headsets);
 - webcams;
 - smart cards and tokens;
 - printing and scanning devices: printers, scanners (including QR code and barcode scanners).

- Centrally manage, update, and monitor Kaspersky Thin Client via the [Kaspersky Security Center Web Console](#). The [Kaspersky Security Management Suite web plug-in](#) is used for communication between Kaspersky Thin Client and Kaspersky Security Center.

Kaspersky Thin Client 2.3 supports Kaspersky Security Center Linux version 15.3 and Kaspersky Security Center Web Console version 15.3.

Kaspersky Thin Client 2.3 supports the following interface languages: Russian, English (USA), Spanish (Mexico), and Portuguese (Brazil).

Distribution kit

Kaspersky Thin Client 2.3 is delivered in one of the following formats:

- Kaspersky Thin Client image without a hardware platform (thin client)
- partner-delivered hardware platform with Kaspersky Thin Client pre-installed

The distribution kit for Kaspersky Thin Client without a hardware platform includes the following files:

- `Kaspersky_Thin_Client_2.3.0.<technical build version>_Wyse3040.tar.gz`—archive containing the installation image of Kaspersky Thin Client for the Dell Wyse 3040 platform.
- `Kaspersky_Thin_Client_2.3.0.<technical build version>_TN1200.tar.gz`—archive containing the installation image of Kaspersky Thin Client for the TONK TN1200 and Centerm F620 platforms.
- `hw_install.sh`—script for installation to the thin client.
- Scripts for updating from the commercial versions 2.0 and 2.01 to version 2.3:
 - `hw_update.sh`
 - `save_files.sh`
 - `restore_files.sh`
- `KTC_LegalNotices_en.txt`—text file containing information about third-party code.
- Text files describing new features and known limitations:
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<technical build version>_EN.txt`
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<technical build version>_ES.txt`
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<technical build version>_PT_BR.txt`
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<technical build version>_RU.txt`
- Kaspersky Thin Client End User License Agreement files:
 - `eula_en_ktc_00008.txt`
 - `eula_es_ktc_00008.txt`

- eula_pt_ktc_00008.txt
- eula_ru_ktc_00008.txt

The distribution kit for Kaspersky Security Management Suite version 2.3 encompasses the components listed below.

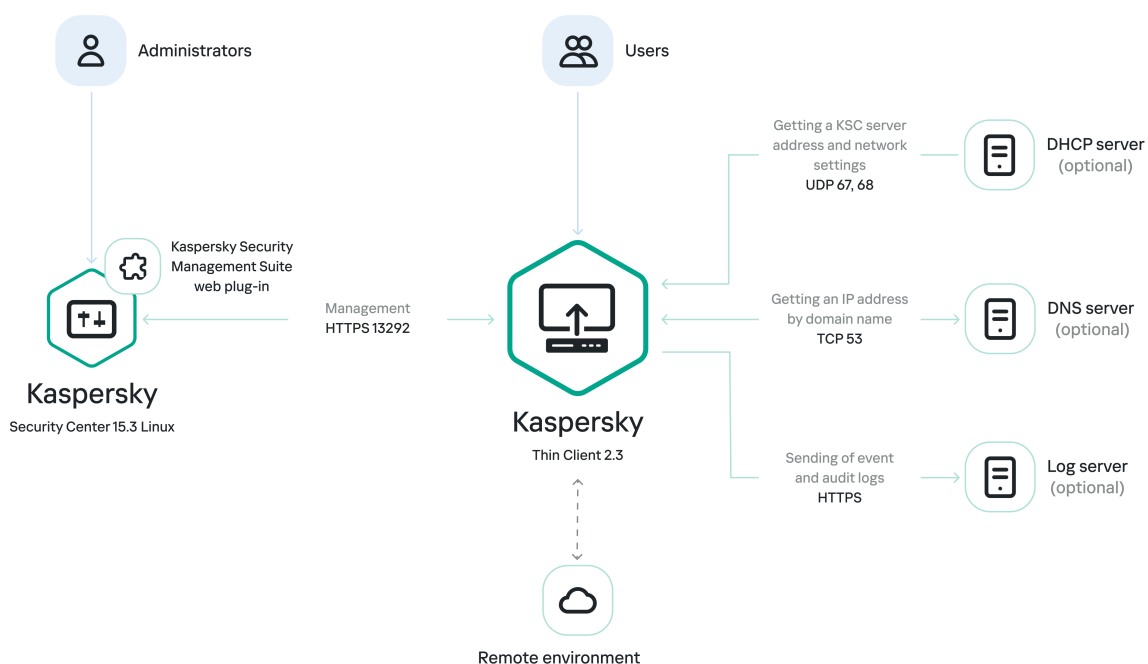
When unpacking the archive using automation tools, such as a script, you must read and accept the terms and conditions of the End User License Agreement before using Kaspersky Security Management Suite.

- Linux archives containing the installation images and web plug-in signature files for Kaspersky Security Center:
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<technical build version>_en.sh
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<technical build version>_es.sh
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<technical build version>_pt_br.sh
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<technical build version>_ru.sh
- Microsoft Windows archives containing the installation images and web plug-in signature files for Kaspersky Security Center:
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<technical build version>_ru.exe
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<technical build version>_en.exe
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<technical build version>_es.exe
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<technical build version>_pt_br.exe
- KSMS_2_3_0_0.conf—RBAC configuration file.
- KSMS_LegalNotices_en.txt—text file containing information about third-party code for Kaspersky Security Management Suite.
- Kaspersky Security Management Suite End User License Agreement files:
 - eula_en_ksms_2.3.rtf
 - eula_es_ksms_2.3.rtf
 - eula_pt_ksms_2.3.rtf
 - eula_ru_ksms_2.3.rtf

Operation of Kaspersky Thin Client

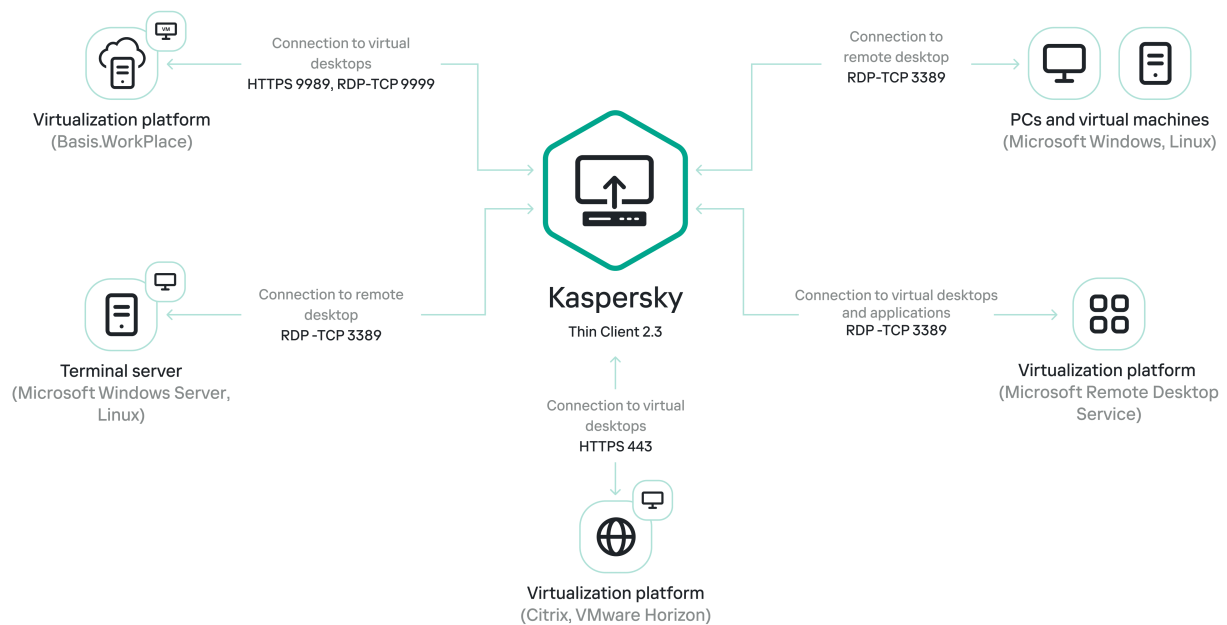
The standard operating scenario for Kaspersky Thin Client (see the figure below) involves the following:

- After Kaspersky Thin Client system is installed on a thin client, 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, and also installs the Kaspersky Security Management Suite [web plug-in](#).
- Kaspersky Thin Client receives trusted certificates, remote environment connection settings, date and time, and other basic settings using a [policy](#) created via Kaspersky Security Center Web Console.
- The user connects to the [remote environment](#).
- In case of problems, the user forwards [audit and event logs](#) via the Kaspersky Thin Client interface to a [log server](#) deployed in your enterprise infrastructure.
- The administrator [updates Kaspersky Thin Client](#).



Standard operating scenario for Kaspersky Thin Client

The image below shows a diagram of Kaspersky Thin Client communication with virtualization platforms and remote environments.



Communication between Kaspersky Thin Client and virtualization platforms and remote environments

Hardware and software requirements

This section describes the hardware and software requirements for Kaspersky Thin Client 2.3.

This document does not provide an overview of thin client hardware components, such as controls and connectors, as this information is available in the vendor documentation for the device where Kaspersky Thin Client is installed.

Monitor requirements

Kaspersky Thin Client supports connection of two monitors.

Depending on the screen orientation settings, Kaspersky Thin Client supports the following monitor resolutions:

- If the screen orientation is set to landscape or landscape flipped:
 - 1024x768 (XGA)
 - 1280x720 (HD)
 - 1280x1024 (SXGA)
 - 1280x768 (WXGA)

- 1440x900 (WXGA+)
- 1400x1050 (SXGA+)
- 1920x1080 (Full HD)
- If the screen orientation is set to portrait or portrait flipped:
 - 1280x1024 (SXGA)
 - 1400x1050 (SXGA+)
 - 1920x1080 (Full HD)

Kaspersky Thin Client supports the following connection interfaces:

- HDMI
- DisplayPort

Kaspersky Thin Client supports only True Color monitors.

Requirements for peripheral devices connected to Kaspersky Thin Client

Kaspersky Thin Client supports the following peripheral devices:

- USB keyboards and mice without multimedia features, and wireless (radio) keyboards and mice.
- USB drives.
- USB smart cards and tokens.
- USB-connected printing and scanning devices: printers, scanners (including QR code and barcode scanners).
A driver for the device connected to the thin client must be installed in the remote environment.
- Wired audio recording and playback devices connected to a mini-jack and via a USB port, and wireless (radio) USB headsets.
- Webcams connected via a USB port.

Requirements for virtualization and remote access systems

Kaspersky Thin Client supports the following virtualization and remote access systems:

- Basis.WorkPlace 2.4.1
- Citrix Virtual Apps and Desktops 2402 cu1
Client: Citrix Workspace app for HTML5 24.11.0.51

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 version 15.3 Linux. 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 the log server

The [log server](#) must meet 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 sends [audit and event logs](#) to the log server using the PUT method.

For instructions on installing and configuring the log server, please refer to the [Knowledge Base](#).

Remote connection methods

This section contains information about remote connection technologies and [remote environments](#) supported by Kaspersky Thin Client, and the ways to connect to these environments using Kaspersky Thin Client applications.

Kaspersky Thin Client uses the following applications:

- **RDP** for connecting to remote desktops or virtual applications via RDP.
- **Basis.WorkPlace** for connecting to virtual desktops deployed in the Basis.WorkPlace infrastructure.
- **Web Access** for connecting to a remote environment deployed in the Citrix Workspace infrastructure.

This section provides information about which of the devices connected to Kaspersky Thin Client can be redirected to a remote environment.

Connecting using the RDP application

In Kaspersky Thin Client, you can connect via RDP to a remote environment, such as Microsoft Remote Desktop Services (MS RDS). The table below describes the available connection methods and peripherals for Windows and Linux operating systems.

Starting with version 2.3.4, Kaspersky Thin Client provides hot plugging of USB tokens, USB drives, and printers (USB) during an active remote connection session.

To redirect peripherals to a Linux remote desktop, install Kaspersky USB Redirector for the xRDP server in the guest operating system. Kaspersky USB Redirector is not included in the distribution kit. You can request the extension from Kaspersky.

Instructions for connecting to a remote environment are given in a [separate article](#).

RDP: supported operating systems, connection methods, and peripherals

	Windows Server 2016/2019/2022 in MS RDS	Windows 10/11	Windows Server 2016/2019/2022	ALT Linux 11 RED OS 8	Astra Linux SE 1.8.1
Connection to a virtual application	✓	✓	✓	—	—
Connection to a remote desktop					
Direct connection	—	✓	✓	✓	✓
Connection using VDI	✓	—	—	—	—
Terminal connection	✓	—	✓	✓	✓
Peripheral devices					
USB tokens	✓	✓	✓	✓ Note	—
Smart cards (USB)	✓	✓	✓	✓ Note	—
USB drives	✓	✓	✓	✓ Note	—
Printers (USB)	✓	✓	✓ Note	✓ Note	—

Scanners (USB)	✓	✓	✓ Note ?	✓ Note ?	—
QR code and barcode scanners (USB)	✓	✓	✓	✓	✓
Microphones (mini-jack, USB) Note ?	✓	✓	✓ Note ?	✓ Note ?	✓ Note ?
Audio playback devices (mini-jack, USB) Note ?	✓	✓	✓ Note ?	✓ Note ?	✓ Note ?
Web camera (video, USB)	✓	✓	✓	—	—

Connecting using the Basis.WorkPlace application

Kaspersky Thin Client can connect to a Basis.WorkPlace remote environment. The table below describes the available connection methods and peripherals for Windows and Linux operating systems.

To redirect peripherals to a Linux remote desktop, install Kaspersky USB Redirector for the xRDP server in the guest operating system. Kaspersky USB Redirector is not included in the distribution kit. You can request the extension from Kaspersky.

Instructions for connecting to a remote environment are given in a [separate article](#).

Basis.WorkPlace: supported operating systems, connection methods, and peripherals

	Windows 10/11	Windows Server 2016/2019/2022	RED OS 8 ALT Linux 11 Astra Linux SE 1.8.1
Connection to a remote desktop			
Direct connection ?	—	—	—
Connection using VDI ?	✓	✓	✓
Terminal connection ?	—	✓	—
Peripheral devices			
USB tokens	✓	✓	—
Smart cards (USB)	✓	✓	—
USB drives	✓	✓	—
Printers (USB)	✓	✓ Note ?	—
Scanners (USB)	✓	✓	—
QR code and barcode scanners (USB)	✓	✓	—
Microphones (mini-jack, USB) Note ?	✓	✓	✓
Audio playback devices (mini-jack, USB) Note ?	✓	✓	✓
Web camera (video, USB)	—	—	—

Connecting using the Web Access application

Using the Web Access application, you can connect to a remote environment deployed in the Citrix Workspace infrastructure. Web Access supports HTML5 and provides a secure HTTPS connection when connecting. The table below describes the specific connection methods and peripheral devices that are available for Windows operating systems.

Connection instructions are provided in a [separate article](#).

Web Access: supported operating systems, connection methods, and peripherals

	Microsoft Windows 10/11	Microsoft Windows Server 2016/2019/2022
Connection to a remote desktop		
Direct connection [?]	—	—
Connection using VDI [?]	✓	✓
Terminal connection [?]	—	✓
Peripheral devices (Citrix Workspace)		
USB tokens	—	—
Smart cards (USB)	—	—
USB drives (FAT16 and FAT32, up to 128 GB)	✓	✓
Printers (USB)	✓	✓
Scanners (USB)	✓	✓
QR code and barcode scanners (USB)	✓	✓
Microphones (mini-jack, USB) Note [?]	✓	✓
Audio playback devices (mini-jack, USB) Note [?]	✓	✓
Web camera (video, USB)	✓	✓

The current version of Kaspersky Thin Client does not support connecting to remote desktops running Linux or using the Web Access application to connect to virtual applications.

When connecting to a remote environment deployed in the Citrix Workspace infrastructure, redirection of more than two USB devices simultaneously is not supported.

What's new

Kaspersky Thin Client version 2.3 has the following new capabilities and improvements:

- Redirection of the following devices to a Citrix virtual environment using the Web Access application:
 - USB drives (via Client Drive Mapping);
 - USB headsets;
 - webcams;
 - printing and scanning devices: printers, scanners (including barcodes and QR codes).
- Redirection of the following devices to a remote environment via RDP:
 - USB headsets;
 - webcams;
 - printing and scanning devices: printers, scanners (including barcodes and QR codes).
- Added the ability to select an audio playback and recording device in the connection panel while in a remote session.
- Added the capability to configure following settings for connecting to a thin client remote desktop via RDP:
 - connection of administrator to thin client remote desktop (automatic, user confirmation, or denied);
 - displaying a user remote session to the administrator: automatically, with user confirmation, or not allowed.
- Support for remote connection to a thin client via the RDP protocol with authorization by device name and password.
- Support for locking the thin client screen from an active remote session.
- Added support for the Dell Wyse 3040 thin client.
- Support for UEFI firmware, which increases the boot speed of the thin client and supports large amounts of memory.
- Added the ability to display on the thin client desktop only those applications that the user has selected in the settings (RDP, Basis.WorkPlace, or Web Access).
- Added the ability to automatically launch one of the applications (RDP, Basis.WorkPlace, or Web Access) as selected by the user, on thin client startup.
- Added the ability to automatically connect to a remote environment after starting RDP.
- Added a language selection wizard for the initial startup of Kaspersky Thin Client.
- Added the ability to set a personalized background on the Kaspersky Thin Client desktop via the Kaspersky Security Center Web Console.

- Added the ability to set a personalized splash screen on the Kaspersky Thin Client lock screen via the Kaspersky Security Center Web Console.
- Added the ability to centrally configure monitors via the Kaspersky Security Center Web Console, including the following settings:
 - screen resolution and orientation
 - display mode (duplicated or extended desktop) of the non-primary screen
- Added the ability to manually define the type of a connected device that the system is unable to recognize.
- Support for redirection of a wireless USB headset, keyboard or mouse (via radio) to a remote environment.
- Added support for the following input languages: German (de-DE), Swiss French (fr-CH), and Swiss German (de-CH).
- Added the ability to pin or completely hide the connection panel in a remote environment.
- Added the ability to [redirect](#) the following tokens via RDP to a RED OS 8.0 remote desktop and then to a Windows 10 remote desktop, as long as a remote desktop session is running between these desktops:
 - Rutoken Lite
 - JaCarta-2 PKI/GOST
- Support for the new version of the [Kaspersky Security Center Web Console](#), 15.3.
- Improved design and text of the user interface of Kaspersky Thin Client and [Kaspersky Security Management Suite](#).

Installing and updating Kaspersky Thin Client

The Kaspersky Thin Client installation procedure depends on the [delivery format](#):

- A partner delivers a hardware platform with Kaspersky Thin Client pre-installed. In that case, installation of Kaspersky Thin Client on the hardware platform is done by TONK.
- Kaspersky Thin Client is delivered without a hardware platform (thin client). In this case, the software platform is installed according to the instructions provided in this section.

Installing Kaspersky Thin Client

Prior to installing Kaspersky Thin Client, do the following:

1. Prepare a bootable USB drive containing the Linux Ubuntu operating system (recommended version: Ubuntu 20.04).
2. Copy the Kaspersky Thin Client installation files received in the [distribution kit](#) to a separate partition on the bootable USB drive or to a separate USB drive:
 - `Kaspersky_Thin_Client_<version number>_Wyse3040.tar.gz` or `Kaspersky_Thin_Client_<version number>_TN1200.tar.gz`—installation image;
 - `hw_install.sh`—Kaspersky Thin Client installation script.

To ensure security prior to installation of Kaspersky Thin Client, we recommend updating the BIOS on the thin client to the latest version, setting a password for BIOS configuration changes, and configuring the option to boot only from a local SSD device. These recommended measures will help prevent potential security risks, such as operating system substitution, replacement or deletion of remote server connection certificates, and unauthorized access to operating system settings.

Kaspersky Thin Client supports Secure Boot technology, which allows UEFI to verify the authenticity of loaded components. If you want to configure Secure Boot, you can get the necessary keys from Kaspersky experts and use the instructions from the [Knowledge Base](#).

To install Kaspersky Thin Client on a thin client:

1. Insert the prepared bootable USB drive into the [appropriate port](#) on the thin client.
2. [Turn on the thin client](#) and boot the Ubuntu image from the bootable USB drive without installing the system on the thin client hard drive.
3. After the operating system loads, go to the directory containing the Kaspersky Thin Client installation files.
4. Run the following command:

```
sudo bash ./hw_install.sh -u Kaspersky_Thin_Client_<version number>_<platform name>.tar.gz
```

where:

- `./hw_install.sh`—path to the installation script;
- `Kaspersky_Thin_Client_<version number>_<platform name>.tar.gz`—installation image.

The *Installed OK! Remove USB drive and reboot* message is displayed after successful installation.

5. Turn off the thin client and extract the bootable USB drive.

The Kaspersky Thin Client system will be loaded the next time you turn on the thin client.

You can check the current OS version number in the [Kaspersky Thin Client interface](#).

Updating Kaspersky Thin Client

You can update Kaspersky Thin Client from version 2.0 or 2.0.1 to version 2.3.

Prior to updating Kaspersky Thin Client, do the following:

1. Prepare a bootable USB drive containing the Linux distribution. We recommend using Linux Ubuntu (recommended version: Ubuntu 20.04).
2. Make sure that the OpenSSL utility is installed on the system. If it is not installed, install it by running the following command:

```
sudo apt install openssl
```
3. Copy the following files from the Kaspersky Thin Client 2.3 distribution kit into one directory on the USB drive:
 - Archive containing the installation image `Kaspersky_Thin_Client_<version number>_TN1200.tar.gz`.
 - Installation and update scripts:
 - `hw_install.sh`
 - `hw_update.sh`
 - `save_files.sh`
 - `restore_files.sh`

To update Kaspersky Thin Client on a thin client:

1. Insert the prepared bootable USB drive into the appropriate port on the thin client.
2. [Turn on the thin client](#) and run the Ubuntu image from the bootable USB drive without installing the system on the thin client hard drive. To do so, select the *Try without installation* option.
3. In the running operating system, go to the directory containing the scripts and the installation image of Kaspersky Thin Client 2.3.

4. Run the update script by using the following command:

```
sudo bash ./hw_update.sh -u <path to the archive containing the installation image of  
Kaspersky Thin Client>
```

If the update script completed successfully, the message *Updated OK!* is displayed.

If an error occurred while the script was running, [contact Technical Support](#).

5. Turn off the thin client and extract the bootable USB drive.

The update is finished. The next time you turn on the device, you will be able to use Kaspersky Thin Client 2.3.

Kaspersky Thin Client interface

The Kaspersky Thin Client interface contains the following elements:

- desktop with applications
- control panel at the top of the window
- connection panel that is displayed during a remote session

Desktop

The central part of the Kaspersky Thin Client desktop displays applications you can use to connect to a [remote environment](#) .

- **RDP**: connect to remote desktops or virtual applications via RDP.
- **Basis.WorkPlace**: connect to virtual desktops deployed in the Basis.WorkPlace infrastructure.
- **Web Access**: connect to a remote environment deployed in the Citrix Workspace infrastructure.

Control panel

The Kaspersky Thin Client control panel contains the following elements:

-  is a shutdown menu button.
In this menu, you can [shut down](#) or [restart](#) Kaspersky Thin Client.
-  is a 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](#)
 - view information about Kaspersky Thin Client updates
 - [view the current End User License Agreement](#)
 - [view information about third-party code](#)
 - [manage access to Kaspersky Thin Client settings](#)
-  is a button for opening the window containing [information about the thin client and Technical Support contacts](#).
- [Status of Kaspersky Thin Client network connection](#) 

-  is a button for opening the [notification panel](#).
- Keyboard [input language switch](#) button.
- [System date and time](#).
-  is a button for opening the [Kaspersky Thin Client remote management](#) menu.

Connection panel

[Connection panel](#) is displayed during a [remote session](#).

The following are displayed in the connection panel while you are connected to a remote desktop:

-  is a button for [closing a remote session](#).
- Connection name.
- Connection status.
-  is a button for opening the window containing [information about the thin client and Technical Support contacts](#).
-  is a button for [locking a remote session](#).
-  is a button for opening the [notification panel](#).
- Network status icon.
-  is a button to open the window for [managing audio playback and recording devices](#).
The button is displayed if two or more devices of this type are connected to the thin client.
-  is a button to open the window for [managing redirection of USB devices](#).
The button is displayed [when connecting to a remote environment deployed in a Citrix Workspace infrastructure](#).

The connection panel additionally displays the following while you are connected to a virtual application:

- application icon
- current date set in Kaspersky Thin Client
- current time set in Kaspersky Thin Client
- Kaspersky Thin Client interface language

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 system.

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 system 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 it. 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 [thin clients](#) 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 thin client:

- [Event log](#) containing technical data on system operation and information about Kaspersky Thin Client events sent to the Kaspersky Security Center Administration Server.
- [Audit log](#) containing the following events and their details:
 - adding, replacing, and switching certificates for connecting to Kaspersky Security Center in the Kaspersky Thin Client interface;
 - factory reset of Kaspersky Thin Client;
 - accepting a remote connection to the thin client;
 - creating a new audit log file in case of log rotation;
 - saving and deleting the user password for auto-connection to a remote environment;
 - enabling (manually and automatically) and disabling management of Kaspersky Thin Client via Kaspersky Security Center.
- System settings:
 - Date and time when Kaspersky Thin Client was installed on the thin client.
 - 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.
 - Location (coordinates) of the connection panel.
 - The previous time certificates were used for authentication when connecting to brokers, remote desktops or virtual applications via RDP, Basis.WorkPlace remote desktops, Web Access remote environments, or a log server.
 - Sound recording and playback device selected as primary.
 - List of applications that are displayed on the Kaspersky Thin Client desktop.
 - Application selected by the user to autostart.
 - List of unrecognized USB devices whose type is defined manually.
 - Lock screen and desktop background files installed on the thin client and their metadata.

- Settings of the connected monitors:
 - primary and secondary monitors
 - primary and secondary monitor ID
 - primary and secondary monitor resolution
 - primary and secondary monitor orientation
 - display mode for a secondary monitor
- Kaspersky Security Center interaction settings:
 - address (name or IP address and port) of the 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;
 - synchronization period between Kaspersky Thin Client and Kaspersky Security Center in minutes;
 - number of certificates received from Kaspersky Security Center for authenticating Kaspersky Thin Client connections to brokers, remote desktops or virtual applications via RDP, Basis.WorkPlace remote desktops, Web Access remote environments, or a log server;
 - current certificate fingerprint for authenticating Kaspersky Thin Client connection to Kaspersky Security Center;
 - thin client naming pattern set by the Kaspersky Security Center administrator (thin client name, ID, and additional details);
 - 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.
- Web Access connection settings:
 - server web address;
 - certificate files for connection authentication;
 - data required for working in the remote environment, such as cookie files.
- 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 broker when connecting to a remote desktop managed by Basis.WorkPlace;

- ID of Kaspersky Thin Client;
- number of reconnection attempts;
- connection profile between Kaspersky Thin Client and the Basis.WorkPlace broker;
- settings for redirecting peripherals to the remote desktop: enabling/disabling redirection of USB drives and smart cards;
- whether use of two monitors is enabled or disabled;
- list of addresses (name or IP address and port) of connection managers of a geographically distributed installation managed by Basis.WorkPlace.
- RDP server connection settings:
 - Address (name or IP address and port) of the Remote Desktop Connection Broker server.
 - Domain and user name for connecting to the Remote Desktop Connection Broker server.
 - Remote Desktop Connection Broker collection ID.
 - Application alias.
 - Certificate files for authenticating the Remote Desktop Connection Broker server when connecting to a remote desktop or virtual application via RDP.
 - Settings for redirecting peripheral devices to the remote desktop:
 - whether redirection of USB drives is enabled or disabled
 - whether redirection of smart cards is enabled or disabled
 - whether redirection of printers is enabled or disabled
 - whether redirection of audio playback devices is enabled or disabled
 - whether redirection of audio recording devices is enabled or disabled
 - whether redirection of the webcam video stream is allowed
 - whether redirection of scanners is enabled or disabled
 - Whether use of two monitors is enabled or disabled.
 - Whether automatic connection to the remote desktop or virtual application 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 showed while dragging
- whether Microsoft Windows themes are enabled or disabled
- Whether automatic connection to the remote desktop is enabled or disabled:
 - password for connecting to the remote desktop, only if the automatic connection option is selected.
- Thin client RDP connection settings:
 - RDP server certificate;
 - secret;
 - thin client remote desktop connection mode (automatic, user confirmation, or denied);
 - remote content display mode (automatic, user confirmation, 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 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;
 - End User License Agreements in Russian, English, Spanish, and Brazilian Portuguese;
 - information about whether or not the End User License Agreements were accepted;
 - information about the release dates of the End User License Agreements.

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 on and starting Kaspersky Thin Client for the first time

Before you start working with Kaspersky Thin Client, you must connect a mouse, keyboard and monitor to the thin client via the corresponding ports. Kaspersky Thin Client also supports connecting [peripheral devices](#) while the system is running.

This document does not provide an overview of the hardware components of a thin client (including controls and connectors) because this information is already provided in the device vendor's documentation. To find out the specific models of thin clients on which Kaspersky Thin Client can be installed, please refer to the [section containing basic information about Kaspersky Thin Client](#).

To start working with Kaspersky Thin Client, you need to turn on the thin client.

To turn on Kaspersky Thin Client and complete the first startup procedure:

1. Press the power on/off button on the thin client.

Kaspersky Thin Client will start loading on your device. After the system has loaded, it displays a user interface language selection window.

2. Select the necessary interface language and click **Next**.

A window opens to show the text of the [End User License Agreement](#) in your selected language.

3. Please carefully read the text of the End User License Agreement and click **Accept**.

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 it.

The initial launch is now complete and the Kaspersky Thin Client [desktop](#) is displayed.

Whenever you turn on the thin client again in the future, the desktop will be displayed after the system loads.

Restarting and turning off Kaspersky Thin Client

When you are finished working with Kaspersky Thin Client, you must turn off the thin client.

To turn off Kaspersky Thin Client:

1. On the Kaspersky Thin Client desktop's control panel, click the shutdown button .
2. In the menu that opens, select **Shut down**.

Kaspersky Thin Client will be turned off.

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

To restart Kaspersky Thin Client:

1. On the Kaspersky Thin Client desktop's control panel, click the shutdown button .
2. In the menu that opens, select **Restart**.

Kaspersky Thin Client will be restarted.

Using certificates in Kaspersky Thin Client

The [TLS encryption protocol](#) ensures secure data transfer between a client and a server 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.

In Kaspersky Thin Client, certificates are used for the following purposes:

- [Connecting a thin client to Kaspersky Security Center](#).
- Connecting to a remote environment:
 - authentication of the Remote Desktop Connection Broker server when connecting to a remote desktop or virtual application
 - authentication of the broker when connecting to a remote desktop managed by Basis.WorkPlace
 - authentication of the server address when connecting to a remote environment in Web Access
- Connecting to a log server.

The user can independently [accept or reject a certificate in the Kaspersky Thin Client interface](#) if the following conditions are met:

- The user is connecting to a [remote environment](#) or to a [log server](#) in the Kaspersky Thin Client interface for the first time.
- The thin client is in one of the following states:
 - not connected to Kaspersky Security Center
 - not added to the administration group
 - [no certificates for connecting to the remote environment have been added](#) for the administration group to which the thin client belongs

All accepted certificates will be saved in the thin client certificate store. In this case, a user could also connect to nodes and use certificates that are not controlled by the administrator.

We recommend [configuring the Kaspersky Thin Client connection](#) to a log server and to a remote environment only using certificates that were assigned by the administrator in the Web Console. In this case, all certificates that were previously accepted by a user will be removed from the thin client certificate store. These measures will help prevent Kaspersky Thin Client from connecting to untrusted nodes.

We advise to update the assigned 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 does not check to see if the certificate is on the Certificate Revocation List.

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 to configure Kaspersky Thin Client and Kaspersky Security Center, and to establish a connection between them. These steps must be performed by the administrator or another qualified expert from your organization who can verify the authenticity of the accepted certificate used to connect to Kaspersky Security Center.

Instructions on installing Kaspersky Thin Client to a thin client are provided in a [separate article](#).

Before installation of Kaspersky Thin Client or prior to the first startup of a thin client on which a Kaspersky Thin Client system is pre-installed, you are advised to update the BIOS on the thin client to the latest version, set a password for BIOS configuration changes, and configure the option to boot only from a local SSD device. These recommended measures will help prevent potential security risks, such as operating system substitution, replacement or deletion of remote server connection certificates, and unauthorized access to operating system settings.

Kaspersky Thin Client supports Secure Boot technology, which allows UEFI to verify the authenticity of loaded components. If you want to configure Secure Boot, you can get the necessary keys from Kaspersky experts and use the instructions from the [Knowledge Base](#).

The scenario for initial configuration of Kaspersky Thin Client and Kaspersky Security Center, and for establishing 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 [Kaspersky Security Center Online Help](#).

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](#).

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 more information about enabling a TCP port on the Kaspersky Security Center Administration Server, please refer to the [Kaspersky Security Center Online Help](#).

5 Turning on Kaspersky Thin Client

[Turn on Kaspersky Thin Client](#) and wait for the system to load. Select the system language. 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 a thin client running Kaspersky Thin Client to an administration group

In the Web Console, [add the thin client to the administration group](#) manually, or set up automated transfer of devices.

9 Creating an active policy in Kaspersky Security Center

In the Web Console interface, [create an active policy](#) for the administration group.

10 Assigning certificates for an administration group

[Assign certificates](#) to connect an administration group to a remote environment and to a log server. We also recommend [adding a certificate](#) for connecting Kaspersky Thin Client to Kaspersky Security Center.

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

Scenario: certificate assignment for a group of thin clients

If certificates are assigned for an [administration group](#) in the Kaspersky Security Center Web Console, a user of a thin client that is included in this group will be able to connect only to the servers for which certificates have been added in the Web Console.

[Kaspersky Security Center must be installed and configured](#) in advance.

The scenario for assigning certificates to a group of thin clients includes 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 Adding thin clients to the administration group

In the Web Console interface, [add a thin client to the administration group](#) if the thin client is still in the unassigned devices group.

3 Creating an active Kaspersky Security Center policy for Kaspersky Thin Client

In the Web Console interface, [create an active policy](#) for the relevant administration group.

4 Adding certificates for connection to a remote environment and a log server

In the Kaspersky Security Center Web Console interface, [add required certificates](#) 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. You can define the synchronization period when configuring Kaspersky Thin Client via the Kaspersky Security Center Web Console. After synchronization, devices will receive the Kaspersky Security Center Administration Server certificates.

If you [remove all certificates](#) that were assigned to a group of devices, the users of thin clients from this group will be able to connect to any server, including servers that have not been assigned any certificates.

Scenario: thin client migration to a new Kaspersky Security Center Server

This section describes the steps to be performed by the administrator when configuring devices running Kaspersky Thin Client for management via a new Kaspersky Security Center Administration Server (hereinafter also referred to as "the Server") if these devices were previously managed via a different Kaspersky Security Center Server.

The scenario for configuring Kaspersky Thin Client management when migrating thin clients to a new Kaspersky Security Center Server 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 [Kaspersky Security Center Online Help](#).

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.

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 more information about enabling a TCP port on the Kaspersky Security Center Administration Server, please refer to the [Kaspersky Security Center Online Help](#).

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 Kaspersky Security Center Server.

7 Updating the security certificate for connecting to Kaspersky Security Center

[Issue a certificate](#) that has to be saved on the current Kaspersky Security Center Administration Server as a reserve one, and then used on the new Server as the primary certificate.

8 Configuring a connection between Kaspersky Thin Client and the new Kaspersky Security Center Server

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.

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](#).

Thin client administration groups are connected to the new Kaspersky Security Center Server, and you can manage them using the Web Console interface.

Configuring general settings

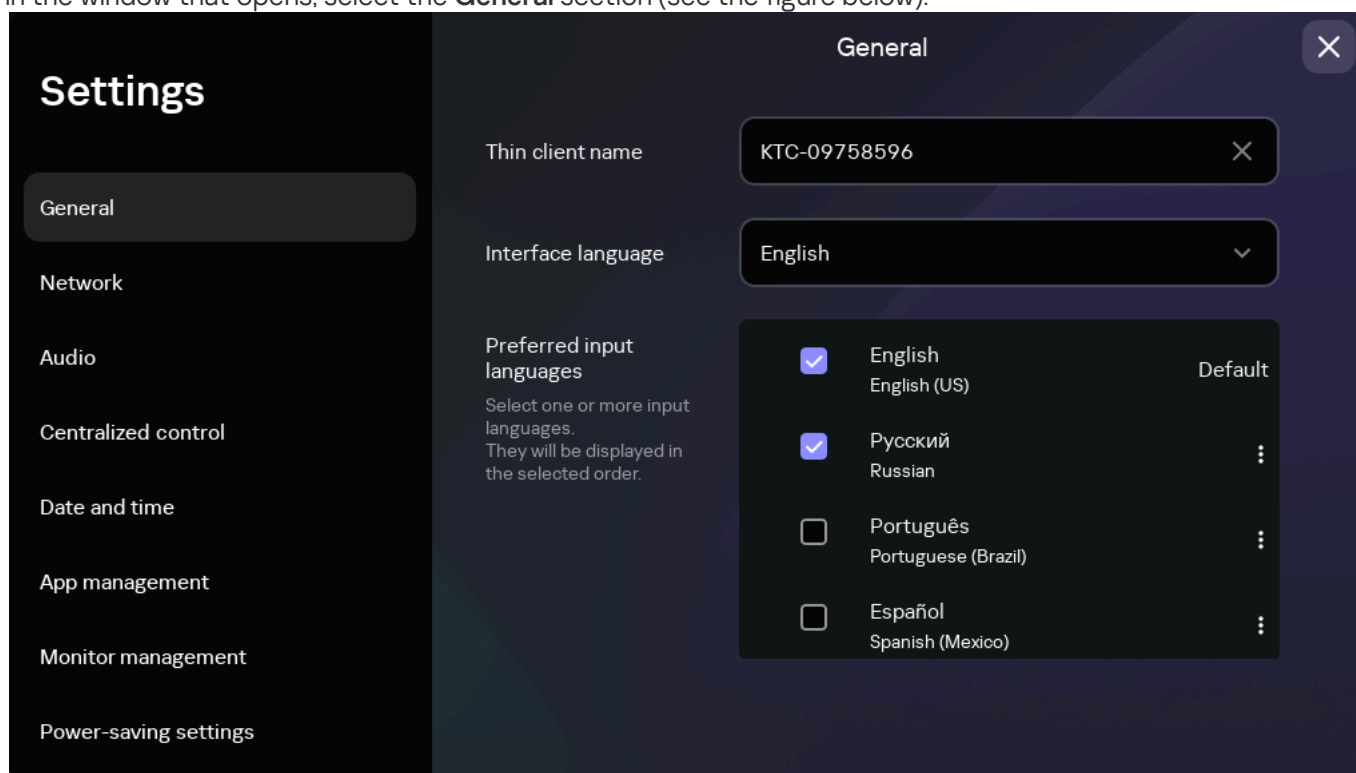
In the Kaspersky Thin Client interface, you can configure the general settings of the thin client. For example, you can specify the thin client name that will be displayed in the Kaspersky Thin Client taskbar and in the Kaspersky Security Center Web Console, and select the language of the Kaspersky Thin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

If the thin client is included in an [administration group](#), the values of settings specified in this article may be enforced through the Web Console. If this is the case, you will not be able to configure these settings in the Kaspersky Thin Client interface.

The settings specified in this article may be [hidden in Kaspersky Thin Client](#).

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).



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** list, select a user interface language. Kaspersky Thin Client 2.3 supports the following interface languages: Russian, English (USA), Spanish (Mexico), and Portuguese (Brazil).
5. In the **Preferred input languages** drop-down list, select one or more languages. Kaspersky Thin Client supports the following input languages: English (USA), Russian, Spanish (Mexico), German (Standard and Switzerland), Portuguese (Brazil), and French (Switzerland). The selected languages are displayed in the Kaspersky Thin Client control panel in the order that you selected, and available when switching the keyboard input language.

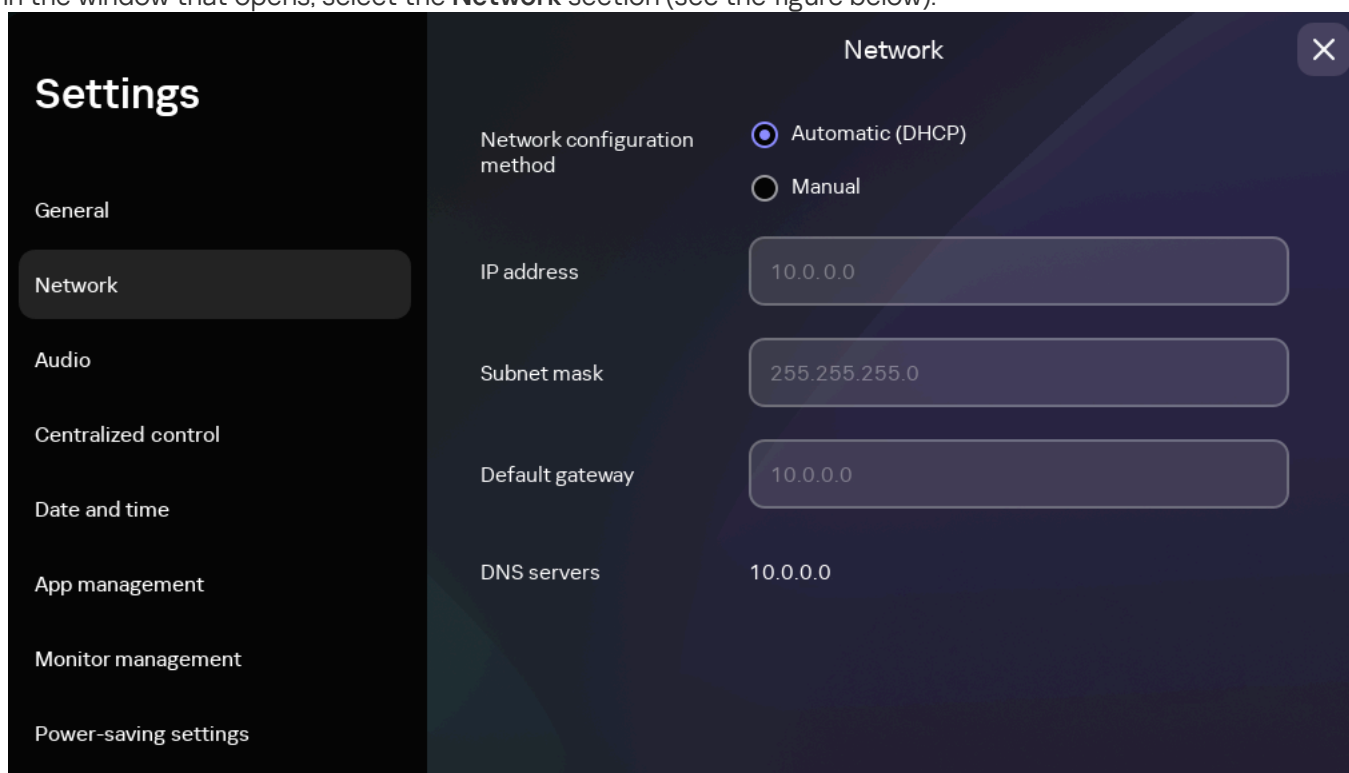
Changes will be applied after the [thin client restart](#).

Configuring network settings

In the Kaspersky Thin Client interface, 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).



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

Managing audio playback and recording devices

You can connect several audio playback and recording devices to a thin client running Kaspersky Thin Client via a mini-jack or USB port to redirect these to the remote environment. In the Kaspersky Thin Client interface, you can [switch between connected devices](#).

Audio volume and other settings are managed from the remote environment.

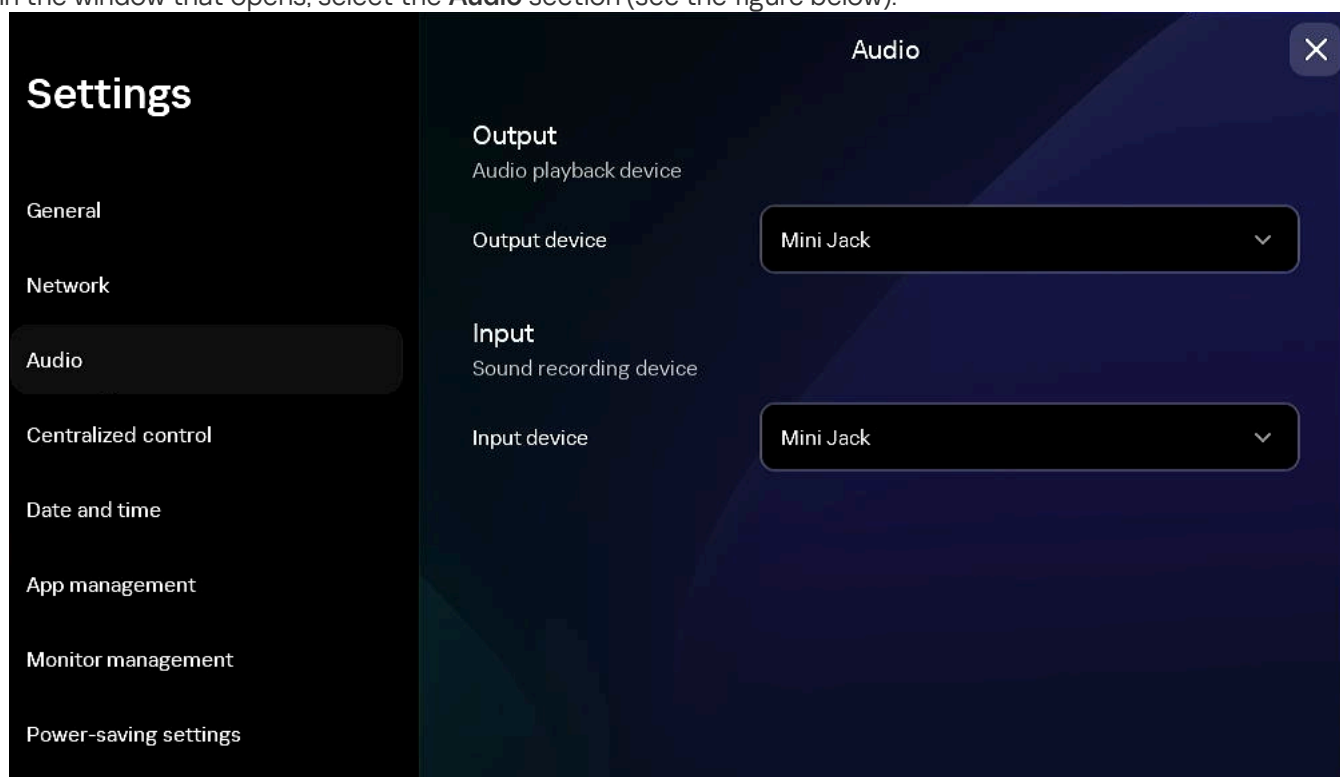
Connection via mini-jack is not supported on Dell Wyse 3040 thin clients.

If the thin client is included in an [administration group](#), the values of settings specified in this article may be enforced through the Web Console. If this is the case, you will not be able to configure these settings in the Kaspersky Thin Client interface.

The settings specified in this article may be [hidden in Kaspersky Thin Client](#).

To select audio playback and recording devices in 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 **Audio** section (see the figure below).



Settings. Audio section

3. In the **Output device** drop-down list, select the audio playback device.
4. In the **Input device** drop-down list, select the audio recording device.

You can also use audio playback and recording devices in the remote environment and [switch between them in the connection panel](#).

Configuring settings for connecting Kaspersky Thin Client to Kaspersky Security Center

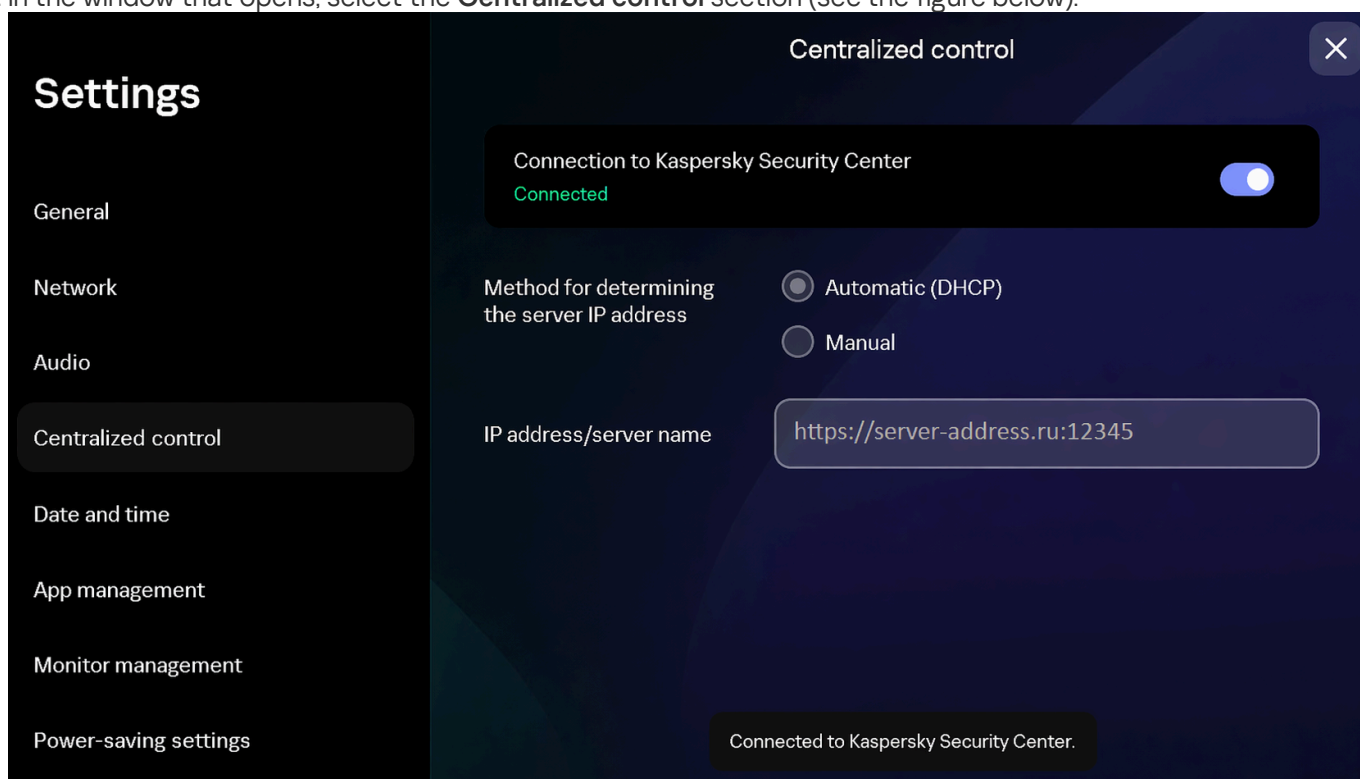
To manage a thin client via the Web Console, you must configure settings for connecting Kaspersky Thin Client to the Kaspersky Security Center Administration Server (hereinafter also referred to as simply "Kaspersky Security Center").

We advise to configure the connection of Kaspersky Thin Client to Kaspersky Security Center with the help of one of your company's qualified experts who will be able to verify the authenticity of the accepted certificate.

We recommend using a separate Kaspersky Security Center Administration Server to manage thin clients in order to receive important security updates from the Kaspersky update servers. The reason for this is that one Kaspersky Security Center Administration Server can have only one active [update task](#) with one priority update source.

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).



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 **Add 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.

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.

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 the thin client is included in an [administration group](#), the values of settings specified in this article may be enforced through the Web Console. If this is the case, you will not be able to configure these settings in the Kaspersky Thin Client interface.

The settings specified in this article may be [hidden in Kaspersky Thin Client](#).

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.

Configuring the date and time

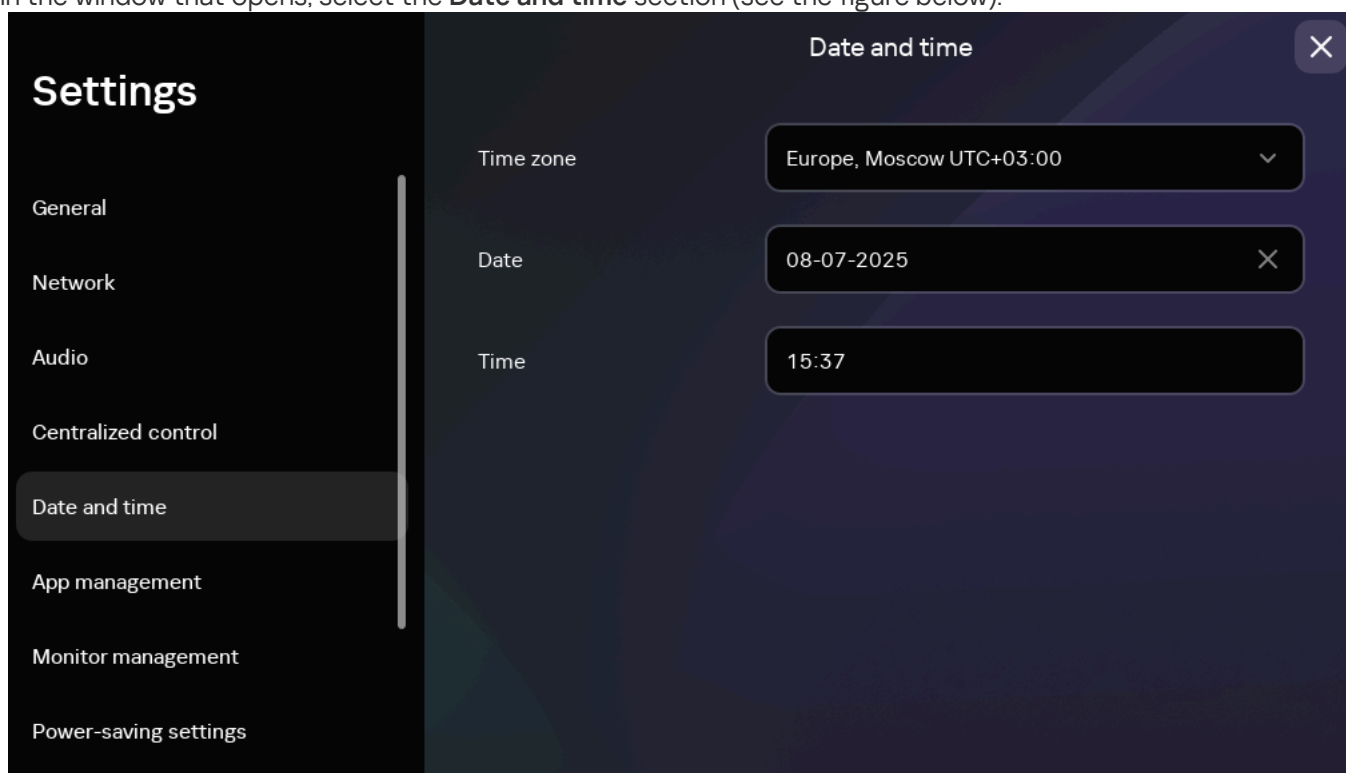
When a thin client is connected to Kaspersky Security Center, it receives the date and time from the Kaspersky Security Center Administration Server. You can manually change the date and time of Kaspersky Thin Client only if the system is not being managed via Kaspersky Security Center.

If the thin client is included in an [administration group](#), the values of settings specified in this article may be enforced through the Web Console. If this is the case, you will not be able to configure these settings in the Kaspersky Thin Client interface.

The settings specified in this article may be [hidden in Kaspersky Thin Client](#).

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).



Settings. Date and time section

3. Configure the date and time settings:

- Select the relevant time zone from the **Time zone** drop-down list.
- In the **Date** field, enter the current date in DD-MM-YYYY format.
- In the **Time** field, enter the current time in HH:MM:SS format.

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

Configuring automatic startup and display of applications

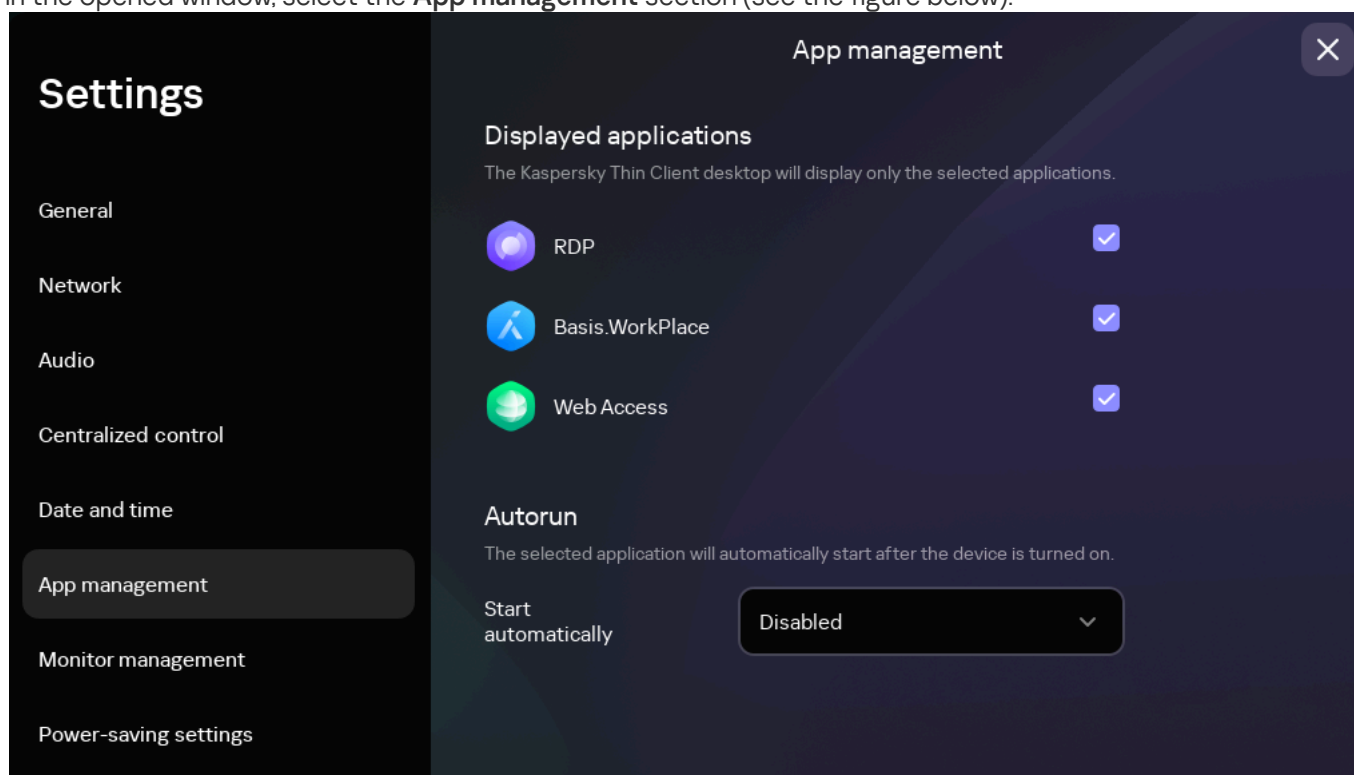
You can select an [application](#) that will be automatically started after starting the device and booting the system, and you can specify which applications will be displayed on the Kaspersky Thin Client desktop.

If the thin client is included in an [administration group](#), the values of settings specified in this article may be enforced through the Web Console. If this is the case, you will not be able to configure these settings in the Kaspersky Thin Client interface.

The settings specified in this article may be [hidden in Kaspersky Thin Client](#).

To configure automatic startup and display of applications:

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



Settings. App management section

3. In the **Displayed applications** block, select the check boxes next to the applications that will be displayed on the Kaspersky Thin Client desktop.
4. In the **Start automatically** drop-down list, select the application that will be automatically started after turning on the device and booting the system. If you select **Disabled**, automatic startup will be turned off.

The changes will be saved and applied.

You can also [configure auto-connection to a remote environment in the RDP application](#) to start a remote session after booting Kaspersky Thin Client.

Configuring monitors and screens

Kaspersky Thin Client supports connection of two monitors.

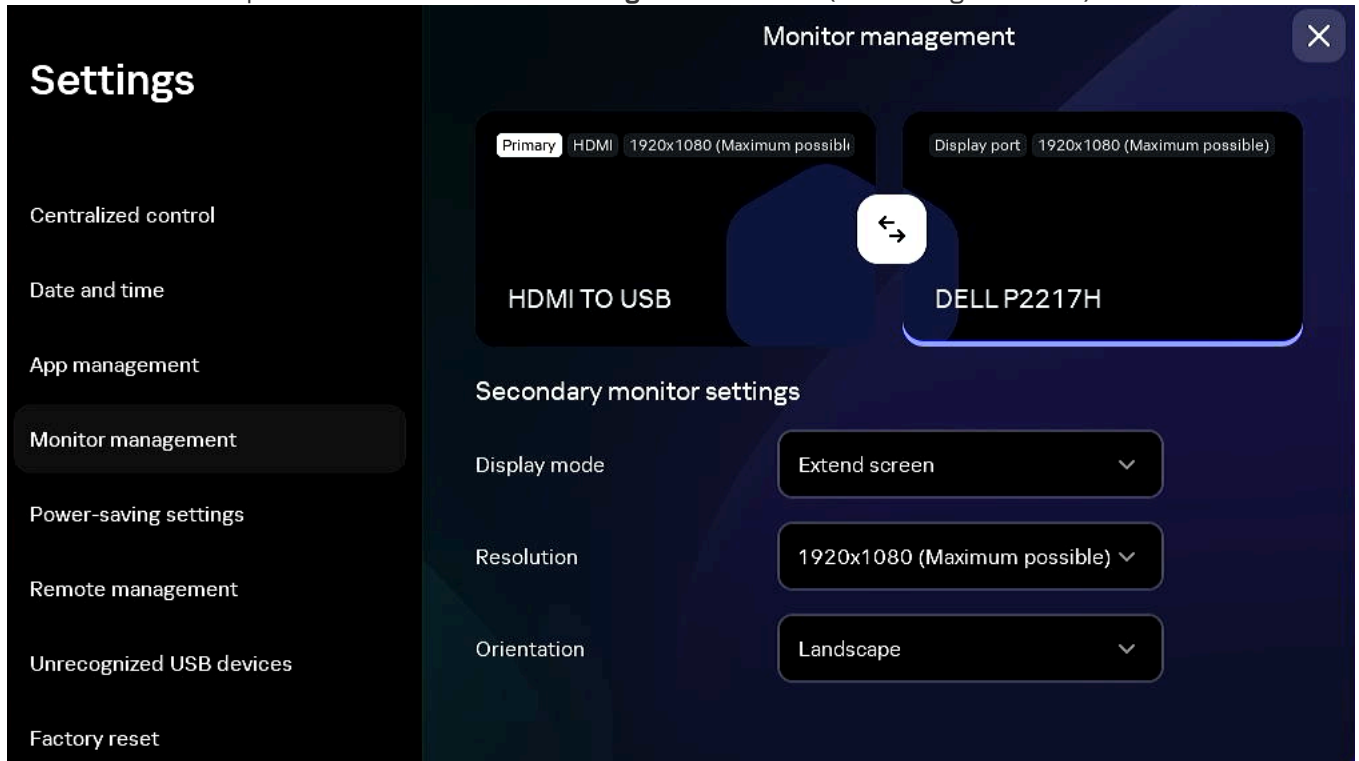
When two monitors are connected, the system considers one as primary and the other as secondary. During a [remote session](#), the connection panel is displayed on the primary monitor screen. The secondary monitor screen extends or duplicates the image of the primary monitor. In the Kaspersky Thin Client interface, you can select which monitor should be considered primary (hereinafter also "change the monitor layout").

If you want the remote session screen to be displayed on both monitors, enable them in the remote environment connection settings in the [RDP](#) or [Basis.WorkPlace](#) applications.

In the Kaspersky Thin Client interface, you can view information about monitors connected to the thin client and change the display layout of their screens, as well as configure the screen settings for each monitor separately.

To set up monitors and screens:

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).



Settings. Monitor management section

3. If you have two monitors connected to your thin client, you can change their layout. To do this, click the  button.
4. If you want to customize the screen of a specific monitor, select the monitor. To do this, click its schematic image.
To highlight the monitor you are going to customize, hover over the schematic image of the monitors. A red frame appears on the customized monitor image.
5. Configure the required settings:
 - In the **Display mode** drop-down list, select the image display option:
 - **Extend screen**—the image spans across two monitors.
 - **Duplicate screen**—the image of the primary monitor's screen is duplicated on the secondary one. If this option is selected, the settings listed below are not available for the additional display.

This option is only displayed if two monitors are connected to the thin client.

- In the **Resolution** drop-down list, select the desired resolution for the selected screen.
Supported resolutions are listed [in the hardware and software requirements section](#).

If the **Maximum possible** value is selected, the highest value of the parameter supported by the monitor and Kaspersky Thin Client is set.

- In the **Orientation** drop-down list, select the screen position:
 - **Landscape**: the standard screen position.
 - **Landscape flipped**: the screen is rotated 180°.
 - **Portrait**: the screen is rotated 90°.
 - **Portrait flipped**: the screen is rotated 270°.

As you change each setting, a countdown window will be displayed.

6. In the window that appears, confirm the changes by clicking **Save**. If you want to discard your changes and return to customizing your settings, click **Cancel**.

The changes will be saved.

Configuring power-saving settings

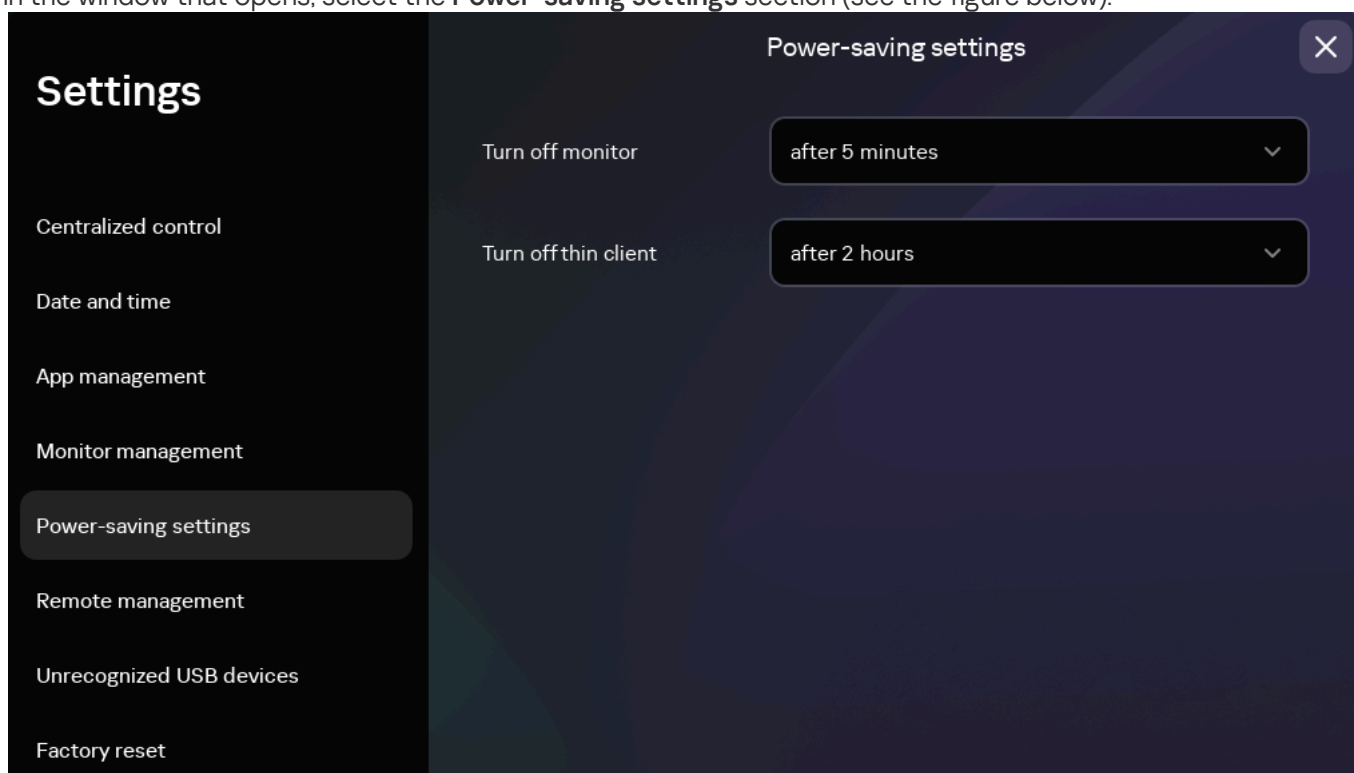
If the thin client is included in an [administration group](#), the values of settings specified in this article may be enforced through the Web Console. If this is the case, you will not be able to configure these settings in the Kaspersky Thin Client interface.

The settings specified in this article may be [hidden in Kaspersky Thin Client](#).

You can configure an idle timeout period to turn off the monitor. 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 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 **Power-saving settings** section (see the figure below).



Settings. Power-saving settings section

3. In the **Turn off monitor** drop-down list, select the system inactivity period after which the monitor will be turned off.
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 settings via the Kaspersky Security Center Web Console.

Configuring remote thin client management settings in the Kaspersky Thin Client interface

If the thin client is included in an [administration group](#), the values of settings specified in this article may be enforced through the Web Console. If this is the case, you will not be able to configure these settings in the Kaspersky Thin Client interface.

The settings specified in this article may be [hidden in Kaspersky Thin Client](#).

In the Kaspersky Thin Client interface, you can configure the following [remote management](#) settings:

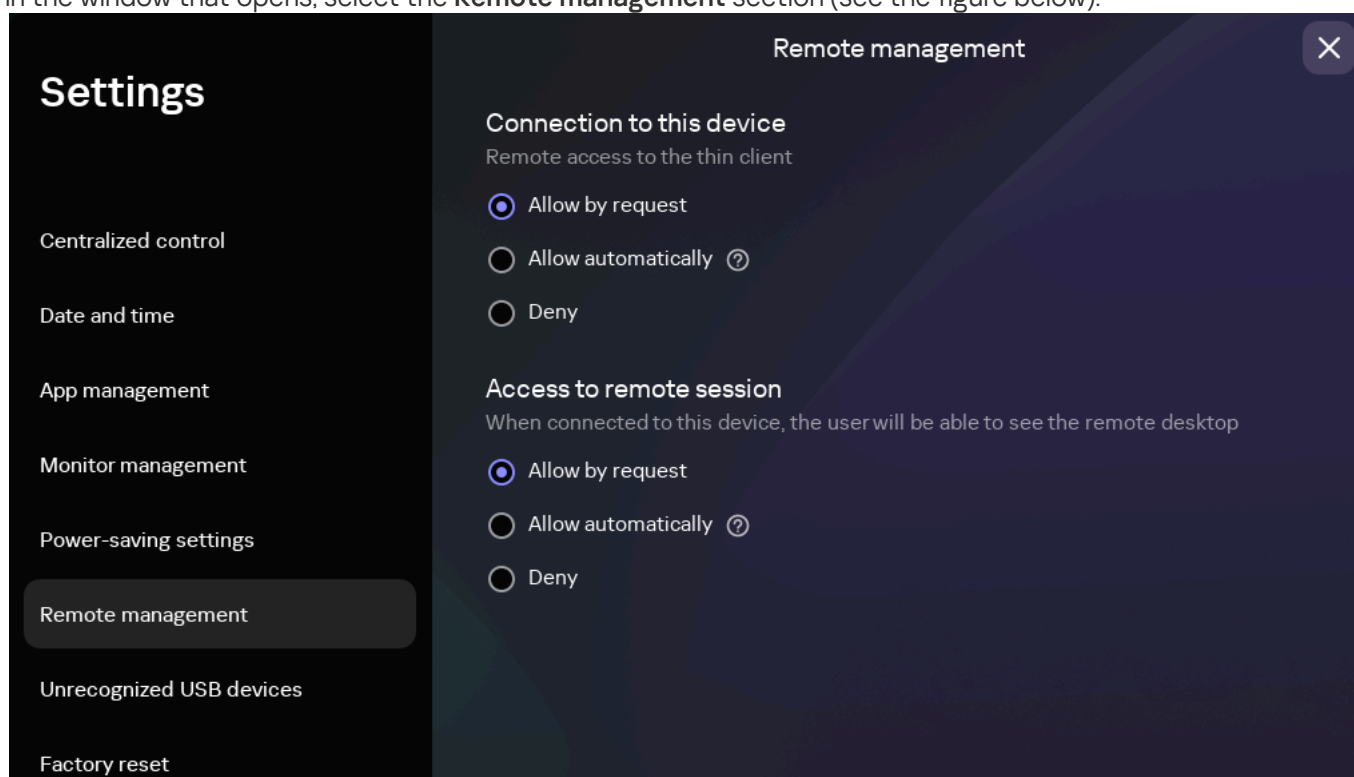
- Remote management access mode.
Defines the conditions and procedure for connecting to a thin client.

- The mode of access to the remote session running on the thin client when the connection to it is established (hereinafter also referred to as the "remote environment screen").

It may be necessary to restrict access to the remote environment screen if the thin client user is working with sensitive or confidential data.

To configure the settings for remote management of a thin client:

1. [Turn on the thin client.](#)
2. In the Kaspersky Thin Client control panel, click  and select **Settings** in the menu that opens.
3. In the window that opens, select the **Remote management** section (see the figure below).



Settings. Remote management section

4. In the **Connection to this device** settings group, select the access mode for remote management of the thin client:

- **Allow automatically**

In this mode, the administrator will be able to remotely connect to the thin client after the user [accepts the remote management request in the Kaspersky Thin Client interface](#). If the user rejects the request, the connection is terminated. If there is no response within 30 seconds, the connection is established automatically.

To ensure device security, use this mode only if the thin client is connected to Kaspersky Security Center.

- **Allow by request**

In this mode, the administrator will be able to remotely connect to the thin client only after the user [accepts the remote management request in the Kaspersky Thin Client interface](#). If the user rejects the request, the connection is terminated.

- **Deny**

In this mode, the administrator will not be able to remotely connect to the thin client.

If you set the **Allow automatically** or **Allow by request** mode, the **Access to remote session** settings group will be displayed.

5. In the **Access to remote session** settings group, select the mode of access to the remote environment screen:

- **Allow automatically**

In this mode, after connecting to the thin client, the administrator will be able to access the remote environment screen without user confirmation.

- **Allow by request**

In this mode, after connecting to the thin client, the administrator will be able to access the remote environment screen only after the user [confirms this access request in the Kaspersky Thin Client interface](#).

- **Deny**

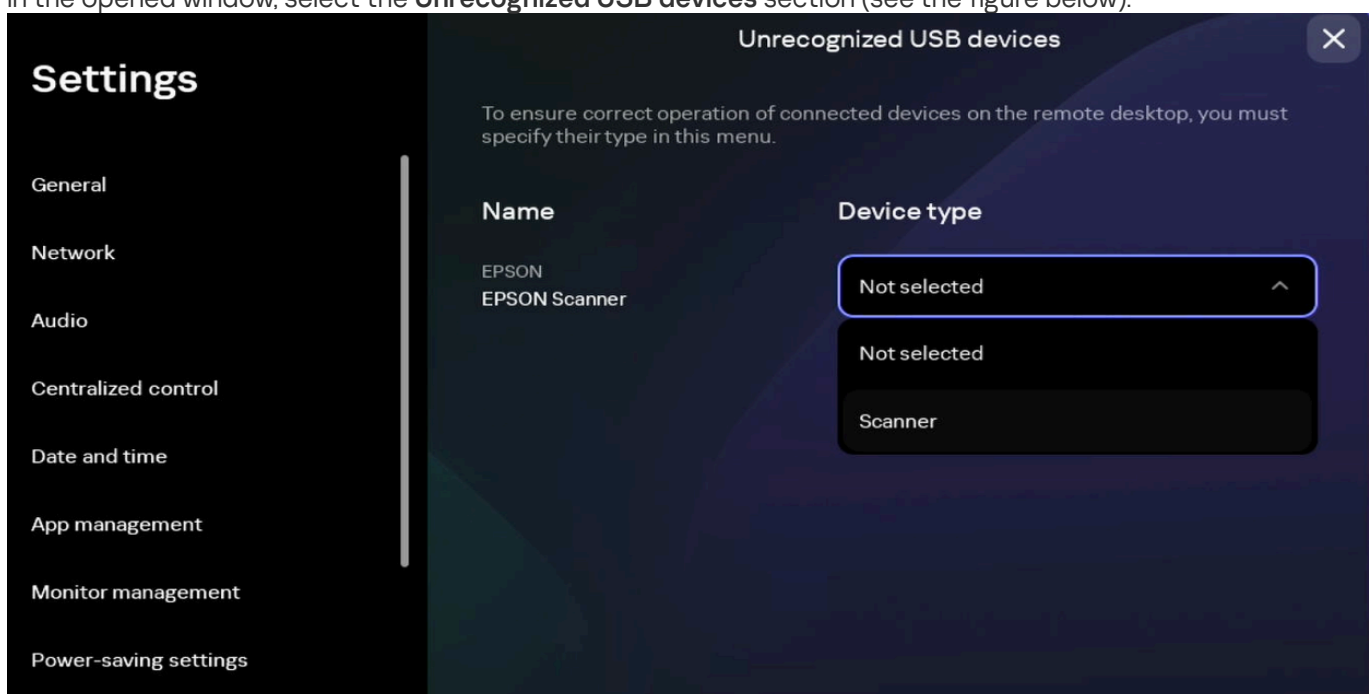
In this mode, the administrator will not be able to remotely manage the thin client until the user manually [terminates the remote session](#).

Changing the type of unrecognized USB devices

By default, Kaspersky Thin Client automatically detects the type of [supported USB device](#) connected to the thin client. If the system fails to determine the type of the connected device (hereinafter also referred to as an "unrecognized device"), you must manually select the type in the Kaspersky Thin Client interface to ensure its correct operation.

To manually change the type of an unrecognized USB device:

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



Settings. Unrecognized USB devices section

You will see a list of USB devices whose types could not be identified by the system. The model name and manufacturer are displayed for each device if the system was able to get this information.

If no unrecognized devices were detected, the list will be empty.

3. In the drop-down list opposite the name of the relevant device, select its type.

In the current version of Kaspersky Thin Client, only the following type of USB device is available: scanner.

The type of unrecognized device will be changed and saved in the system. You can now [redirect the device to a remote environment](#).

Resetting Kaspersky Thin Client settings

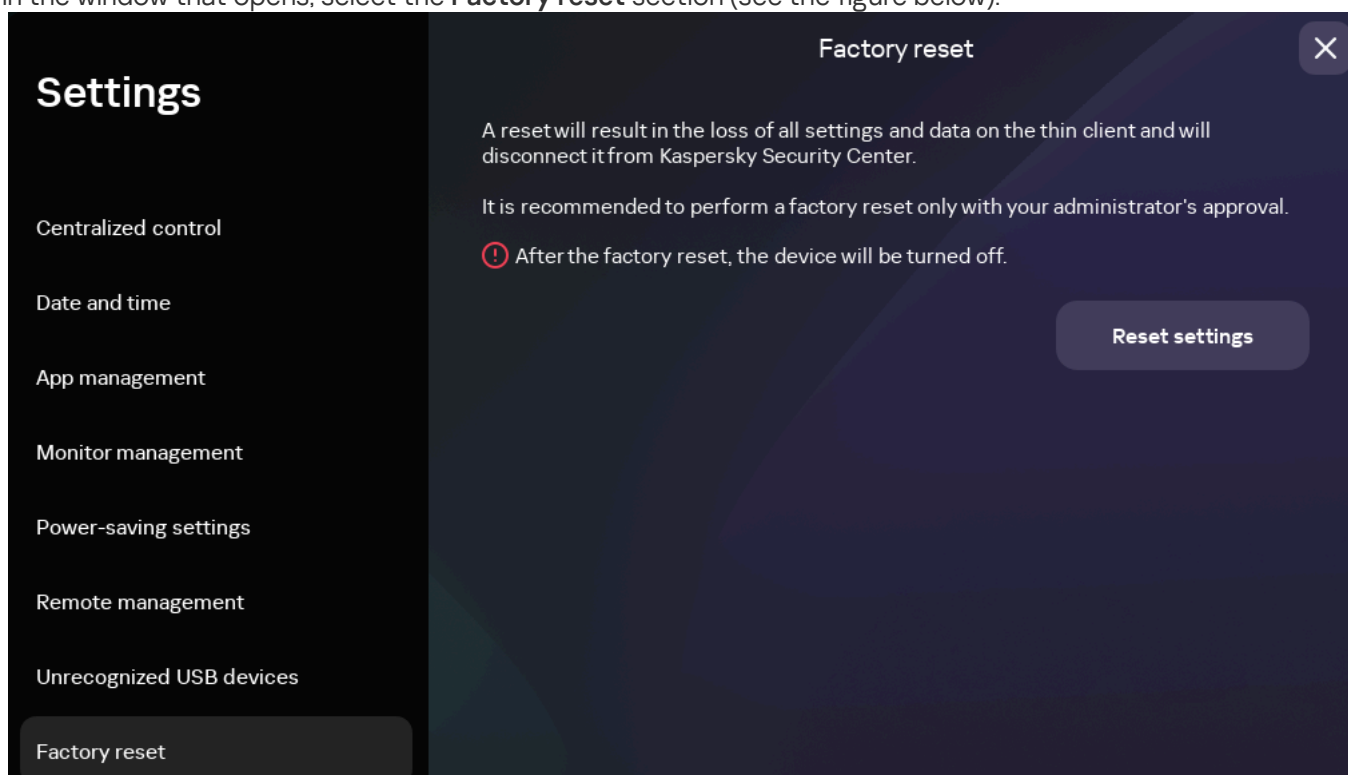
Reset will result in the loss of all defined settings and all data of Kaspersky Thin Client (except the [audit log](#) and system date), and will disconnect the device from Kaspersky Security Center. We recommend performing a reset only after approval with your company administrator.

If the thin client is included in an [administration group](#), the values of settings specified in this article may be enforced through the Web Console. If this is the case, you will not be able to configure these settings in the Kaspersky Thin Client interface.

The settings specified in this article may be [hidden in Kaspersky Thin Client](#).

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).



Settings. Factory reset section

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.

To perform a factory reset of a thin client that is included in an administration group:

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.
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.

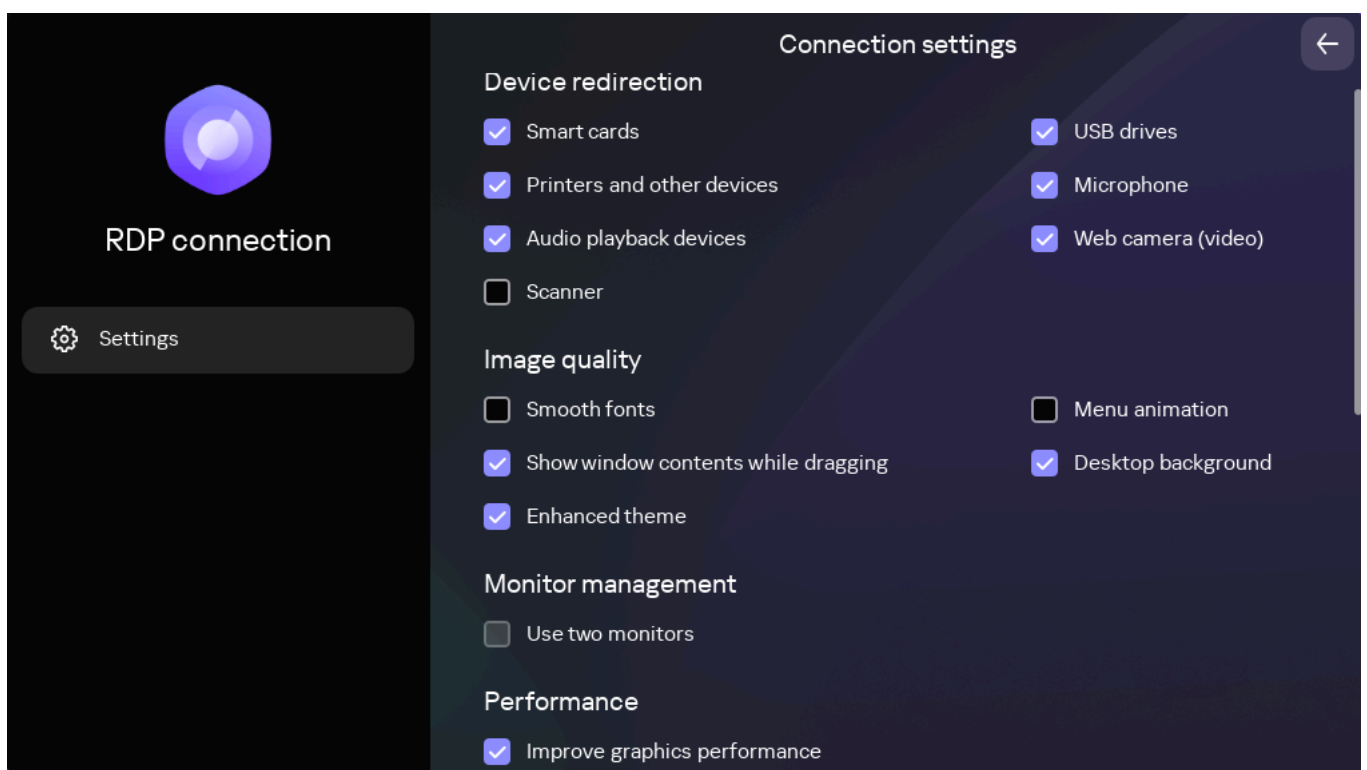
Configuring settings for connecting to a remote environment using the RDP application

In the RDP application, you can configure the settings for [connecting to a virtual application or remote desktop](#) via RDP, including via an automatic connection to a remote environment.

To configure the settings for connecting to a remote environment in the RDP application:

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

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



Window for configuring a connection to a remote environment in the RDP application

3. In the **Device redirection** settings block, select the devices to be redirected to the remote environment: **Smart cards**, **USB drives**, **Printers and other devices**, **Microphone**, **Audio playback devices**, **Web camera (video)**, **Scanner**.

Audio volume and other settings are managed from the remote environment.

To correctly redirect USB devices to a remote desktop in the Windows 10 operating system, you must enable Microsoft Remote Desktop Services and allow redirection of Plug and Play devices in the settings of Remote Desktop Services. For Microsoft Windows Server 2016 and 2019, you must also enable remote connections via Remote Desktop Services and allow setting remote management rules in Remote Desktop Services.

4. In the **Image quality** block, select the check boxes next to the graphic settings of the remote desktop that you want to use: **Smooth fonts**, **Menu animation**, **Desktop background**, **Show window contents while 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.
6. To improve performance when connected to remote desktops or applications, in the **Performance** block, check **Improve graphics performance**.
7. To automatically [connect to a remote desktop or virtual application](#) when the RDP application is started, in the **Auto-connect** block, select the **Connect automatically** check box.

To activate the function, you must manually connect to and disconnect from the remote environment once. When you do so, the following data for connecting to the RDP server is saved in the thin client storage: user name, server address, and password. The next time you start the RDP application, these credentials will be used to automatically initiate a connection to the remote environment. If you disable the auto-connect function, the saved password is deleted from the device storage.

To automatically connect to the remote environment in the RDP application immediately after booting Kaspersky Thin Client, [configure automatic startup of the application](#) in the **Settings** section.

8. If you need 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 need to start a virtual application, specify the application alias in the **Application alias** field.

9. If you want to automatically restore a remote desktop connection that is unexpectedly disconnected, select the **Connect again if connection is lost** check box.
10. Click the back arrow in the upper-right corner of the window to return to the connection window.

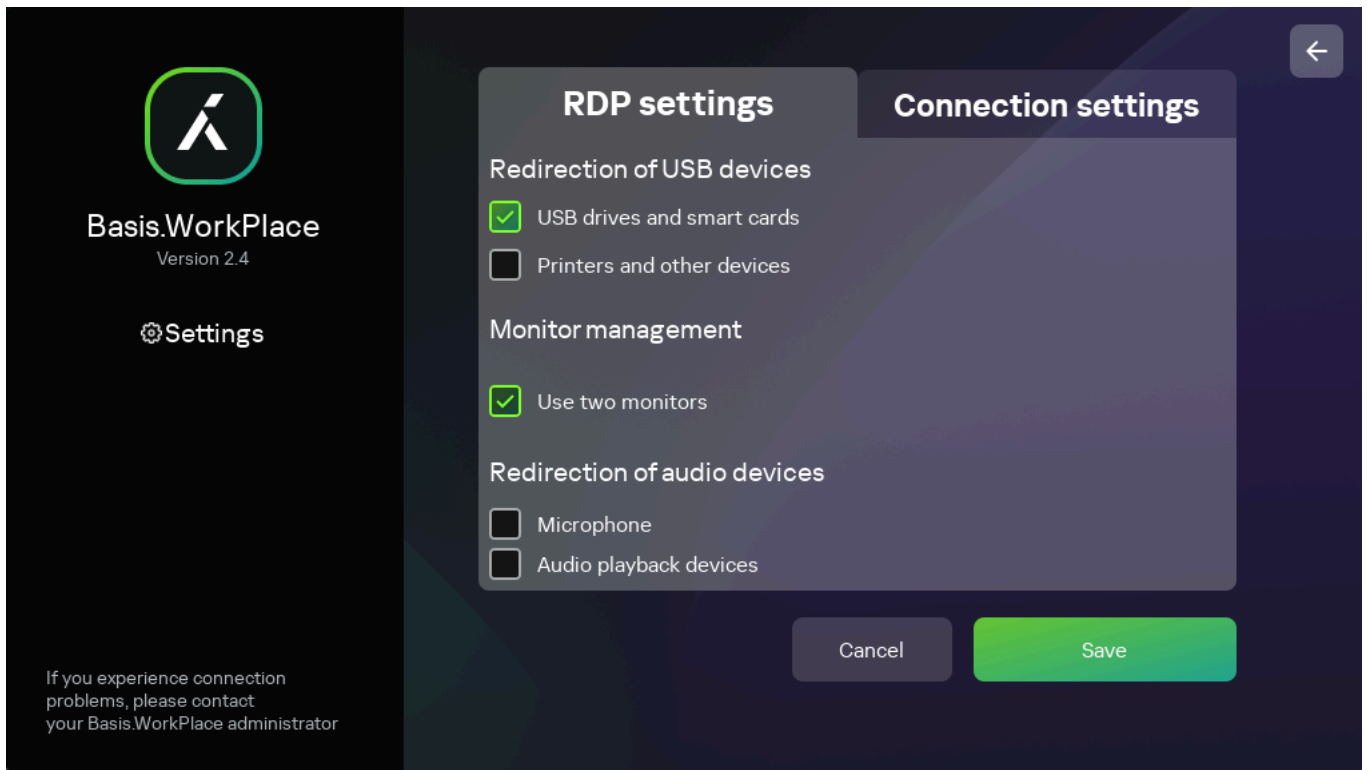
Configuring settings for connecting to a remote environment using the Basis.WorkPlace application

Using the Basis.WorkPlace application, you can configure the settings for connecting to a remote environment deployed in the Basis.WorkPlace infrastructure.

To configure the settings for connecting to a remote environment in the Basis.WorkPlace application:

1. On the Kaspersky Thin Client desktop, 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 the settings for redirecting devices to a remote environment (see the figure below).



Window for configuring redirection of devices to a remote environment deployed in a Basis.WorkPlace infrastructure

3. To configure the settings for redirecting devices to a remote environment:

- a. In the **Redirection of USB devices** settings block, select devices to redirect to the remote environment: **USB drives and smart cards**, **Printers and other devices**.
- b. 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.
- c. In the **Redirection of audio devices** settings block, select devices to be redirected to the remote environment: **Audio playback devices**, **Microphone**.
- d. Audio volume and other settings are managed from the remote environment.

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

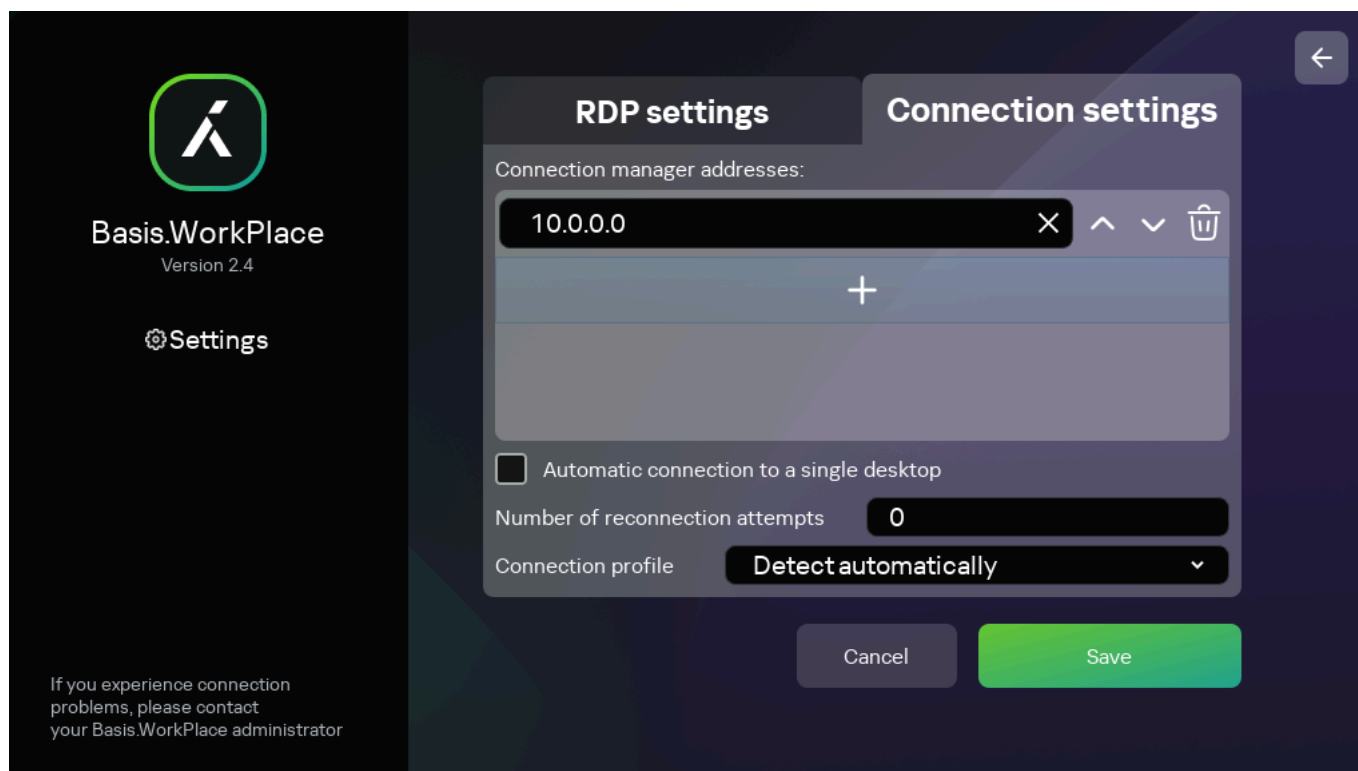
4. To configure the settings for connecting to a geographically distributed remote environment, go to the **Connection settings** tab (see the figure below).

For a detailed description of the settings of this tab, please refer to the [Geo-Distributed Installation Guide](#) on the Basis.WorkPlace website.

Do the following on the selected tab:

- a. In the **Connection manager addresses** section, click + and specify the IP address of the Basis.WorkPlace [broker](#) in the displayed field. You can add no more than four IP addresses.

- b. In the **Number of reconnection attempts** field, enter the number of times that Kaspersky Thin Client should attempt to reconnect to the Basis.WorkPlace broker if disconnected. You can indicate no more than five attempts at reconnection.
- c. In the **Connection profile** drop-down list, select the type of connection between Kaspersky Thin Client and the Basis.WorkPlace 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



Window for configuring a connection to a geo-distributed remote environment deployed in a Basis.WorkPlace infrastructure

5. Click **Save** in the lower part of the window to save the changes.
6. Click the back arrow in the upper-right corner of the window to return to the window for connecting to the remote environment.

Managing access to Kaspersky Thin Client settings

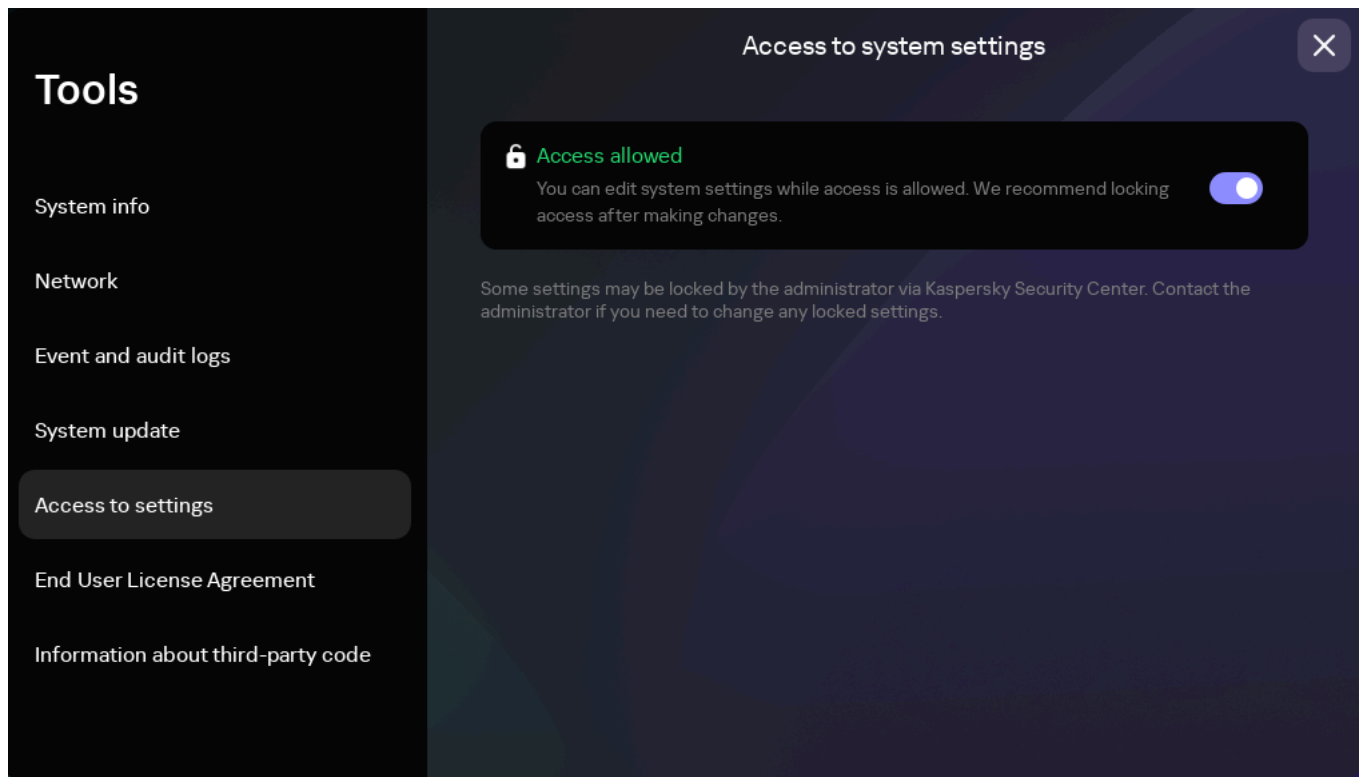
You can configure the Kaspersky Thin Client interface to display or hide settings that are configured only once and are no longer used in the core operating scenarios of the thin client.

If the thin client is included in an [administration group](#), the values of settings may be enforced through the Web Console. These enforced settings will be blocked from editing in the Kaspersky Thin Client interface, and you will not be able to enable or disable their display.

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 locked** position.
All of the following settings will be hidden in the thin client interface:
 - [RDP connection settings](#)
 - [Basis.WorkPlace connection settings](#)
 - [General settings](#)
 - [Network settings](#)
 - [Kaspersky Security Center connection settings](#)
 - [Date and time](#)
 - [Power-saving settings](#)
 - [Layout of monitors](#)
 - [Reset of Kaspersky Thin Client settings](#)

- If you need to display the settings, move the toggle button to the **Access allowed** position. The settings will be displayed. You will be able to define new values for these settings.



Tools. Access to settings section

Managing Kaspersky Thin Client installed on a thin client

This section describes the main Kaspersky Thin Client operating scenario and contains instructions for using Kaspersky Thin Client.

Scenario: working in Kaspersky Thin Client on a thin client

The main scenario for working in Kaspersky Thin Client installed on a [thin client](#) consists of the following stages:

1 Preparing Kaspersky Thin Client for startup

Connect the [peripherals](#) to the thin client before starting it for the first time.

2 Starting Kaspersky Thin Client

[Turn on](#) the thin client to get started.

3 Getting started in a remote session

[Connect to a remote environment](#) and start working in a remote session.

4 Locking and unlocking a remote session

[Lock your remote session](#) if you need to spend some time away from your workstation. Resume work upon returning.

5 Closing a remote connection

[Terminate your remote session](#) when done working.

6 Stopping Kaspersky Thin Client

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

Connection to a remote environment

This section provides information on how to connect to a [remote environment](#) using Kaspersky Thin Client applications and how to start working in a [remote session](#).

The following limitations apply when connecting to a remote environment in Kaspersky Thin Client:

- File exchange between Kaspersky Thin Client and the remote environment is not supported.
- Clipboard sharing between Kaspersky Thin Client and the remote environment is not supported.
- Running multiple remote sessions simultaneously, or connecting to multiple remote environments simultaneously within a single remote session are not supported.

Kaspersky Thin Client uses [TLS](#) encryption (versions 1.2, 1.3) to protect all remote sessions and keep data from being intercepted or spoofed.

To connect to remote environments running Microsoft Windows, Kaspersky Thin Client supports the following cipher suites:

- For TLS 1.2:
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 = {0xC0, 0x30}.
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 = {0xC0, 0x2F}.
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 = {0xC0, 0x2B}.
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 = {0xC0, 0x2C}.
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 = {0xCC, 0xA8}.
 - TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 = {0xCC, 0xAA}.
 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 = {0x00, 0x9F}.
- For TLS 1.3:
 - TLS_AES_128_GCM_SHA256 = {0x13, 0x01}.
 - TLS_AES_256_GCM_SHA384 = {0x13, 0x02}.
 - TLS_CHACHA20_POLY1305_SHA256 = {0x13, 0x03}.
 - TLS_AES_128_CCM_SHA256 = {0x13, 0x04}.

Connecting to a remote environment using the RDP application

In the RDP application, you can connect to [remote desktops](#) and [virtual applications](#) via RDP.

Connection to a remote desktop

To connect to a remote desktop in the RDP application:

1. [Turn on Kaspersky Thin Client](#).
2. On the Kaspersky Thin Client desktop, click the **RDP** button.
3. In the window that opens, specify the connection settings:
 - a. In the **Server** field, specify the IP address or name of the Microsoft Remote Desktop Connection Broker server.

Kaspersky Thin Client saves the last entered server address 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. You can specify the domain user name in Domain\User name format or in User name format.

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

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

If you have not [activated the automatic connection function](#), the password is not saved and you must enter it again the next time you connect.

4. To [configure settings](#) for connecting to a remote desktop, click **Settings** in the left part of the window.

5. Press **Enter** or click **Connect**.

You will see a window prompting you to add a certificate to connect to the remote environment if the following conditions are met:

- You are connecting to a remote environment in the Kaspersky Thin Client interface for the first time.
- The thin client is in one of the following states:
 - not connected to Kaspersky Security Center
 - not added to the [administration group](#) 
 - [no certificates for connecting to the remote environment have been added](#) for the administration group to which the thin client belongs

Check the certificate settings 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.

6. 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.

A remote desktop window opens, and a remote session starts.

Connection to a virtual application

To connect to a [virtual application](#)  in RDP application:

1. [Turn on Kaspersky Thin Client](#).

2. On the Kaspersky Thin Client desktop, click the **RDP** button.

3. In the window that opens, specify the connection settings:

a. In the **Server** field, specify the IP address or name of the Microsoft Remote Desktop Connection Broker server.

Kaspersky Thin Client saves the last entered server address 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. You can specify the domain user name in Domain\User name format or in User name format.

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

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

If you have not [activated the automatic connection function](#), the password is not saved and you must enter it again the next time you connect.

4. Click **Settings** in the left part of the window.

5. In the **Remote Desktop Connection Broker collection ID** field, 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).

6. In the **Application alias** field, specify the alias of the virtual application that you want to open.

Kaspersky Thin Client saves the alias that you entered last, so you do not need to enter it again when reconnecting.

7. Click the back arrow in the upper-right corner of the window to return to the connection window.

8. In the connection window, press **Enter** or click **Connect**.

You will see a window prompting you to add a certificate to connect to the remote environment if the following conditions are met:

- You are connecting to a remote environment in the Kaspersky Thin Client interface for the first time.
- The thin client is in one of the following states:
 - not connected to Kaspersky Security Center
 - not added to the [administration group](#) 
 - [no certificates for connecting to the remote environment have been added](#) for the administration group to which the thin client belongs

Check the certificate settings 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.

A virtual application window opens, and a remote session starts.

To switch to another window of a running virtual application,

hover the mouse over the application icon in the [connection panel](#) in the upper part of the screen and select the relevant window from the drop-down list.

Connecting to a remote environment using the Basis.WorkPlace application

In the Basis.WorkPlace application, you can connect to Basis.WorkPlace virtual desktops.

Users cannot initiate a password change in Kaspersky Thin Client.

To connect to a virtual desktop in the Basis.WorkPlace application:

1. [Turn on Kaspersky Thin Client](#).
2. On the Kaspersky Thin Client desktop, 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 [broker](#) server.

Kaspersky Thin Client saves the address of the Basis.WorkPlace broker with which a connection was successfully established so that 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 user password is not saved; the next time you connect, you will need to enter the password again.

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 virtual desktop connection window. The number of allowed password entry attempts is defined by the active security policy set by the Basis.WorkPlace administrator.

4. Press **Enter** or click **Connect**.

You will see a window prompting you to add a certificate to connect to the remote environment if the following conditions are met:

- You are connecting to a remote environment in the Kaspersky Thin Client interface for the first time.
- The thin client is in one of the following states:
 - not connected to Kaspersky Security Center
 - not added to the [administration group](#)
 - [no certificates for connecting to the remote environment have been added](#) for the administration group to which the thin client belongs

Check the certificate settings 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.

A Basis.WorkPlace infrastructure window will open with available virtual desktops.

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

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

A virtual desktop window will appear. A remote session will start.

An administrator can restrict access to Basis.WorkPlace. For example, they can lock your user account or block access to virtual desktops that were previously accessible to your user account. If you have issues connecting to the remote environment, please contact your organization's administrator.

Connecting to a remote environment using the Web Access application

Using the Web Access application, you can connect to a remote environment deployed in the Citrix Workspace infrastructure. Web Access supports HTML5 and provides a secure HTTPS connection when connecting.

Any data required for remote sessions, such as cookie files, will be retained on the thin client until the remote session is closed. After that, the data will be deleted.

To connect to a remote environment using the Web Access application:

1. [Turn on Kaspersky Thin Client](#).
2. On the Kaspersky Thin Client desktop, click the **Web Access** button.
3. In the connection window that opens, provide the required remote environment server address in the **Server** field.
4. Press **Enter** or click **Connect**.

You will see a window prompting you to add a certificate to connect to the remote environment if the following conditions are met:

- You are connecting to a remote environment in the Kaspersky Thin Client interface for the first time.
- The thin client is in one of the following states:
 - not connected to Kaspersky Security Center
 - not added to the [administration group](#) 
 - [no certificates for connecting to the remote environment have been added](#) for the administration group to which the thin client belongs

Check the certificate settings 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.

The connection data input window is displayed.

5. Enter the user name and password for connecting to the remote environment.

The system does not save the credentials for connecting to a remote environment deployed in a Citrix Workspace infrastructure, therefore you must enter them every time you start a remote session.

If one remote desktop is available to you, it will be displayed on the screen and you can start working in the remote environment. If several remote desktops are available to you, you will see a window containing a list of them.

6. To refresh the list of remote desktops, click the **Reload** button.

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

A window of the remote environment you are connected to will appear. A [remote session](#) will start.

Managing a remote session

This section contains information on how to manage a [remote session](#) in the Kaspersky Thin Client interface using the connection panel and [hotkeys](#).

Using the connection panel

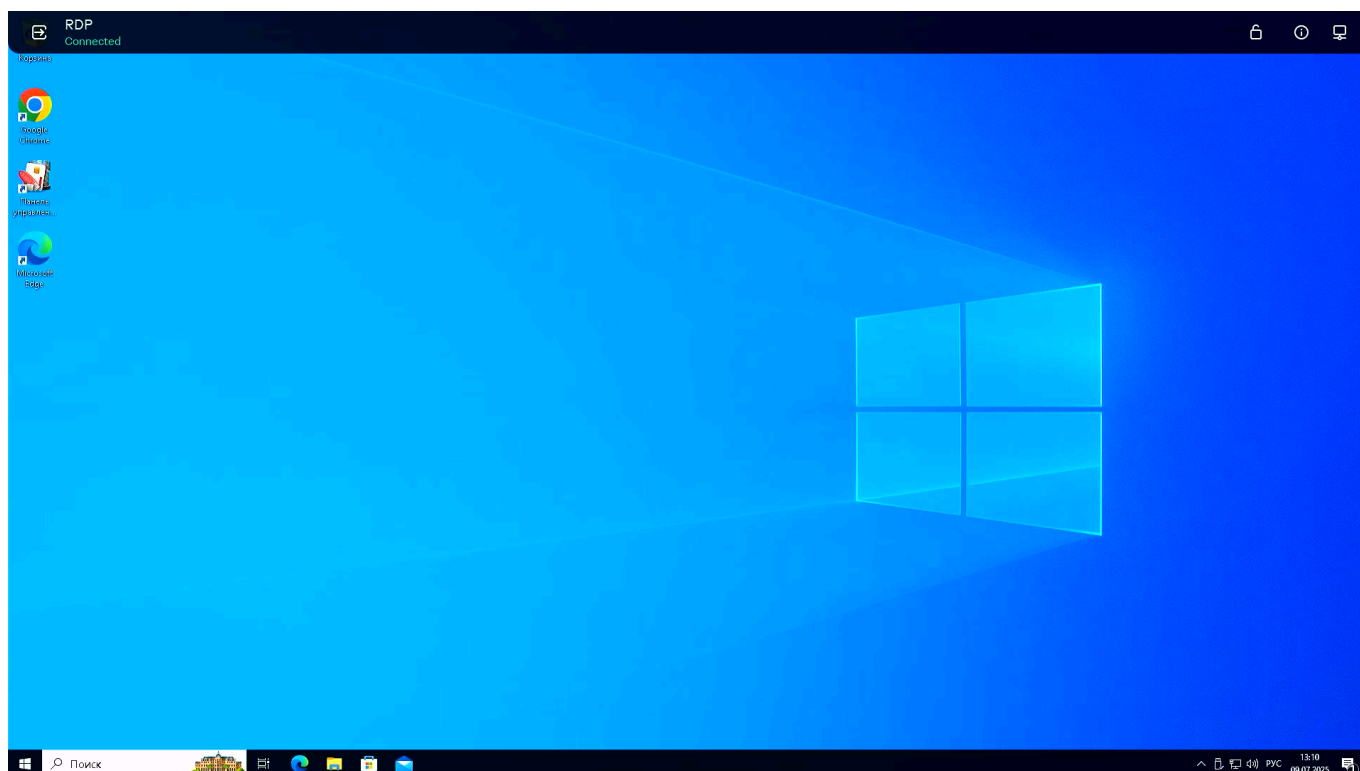
The connection panel (hereinafter also referred to as "the panel") is displayed in the upper part of the screen after you successfully connect to a remote environment. It is used for managing the active [remote session](#).

Connection panel states

The connection panel can be in one of the following states:

- Expanded.

The panel is fully displayed in the upper part of the remote session screen (see the figure below).



Window showing a running remote session with the expanded connection panel

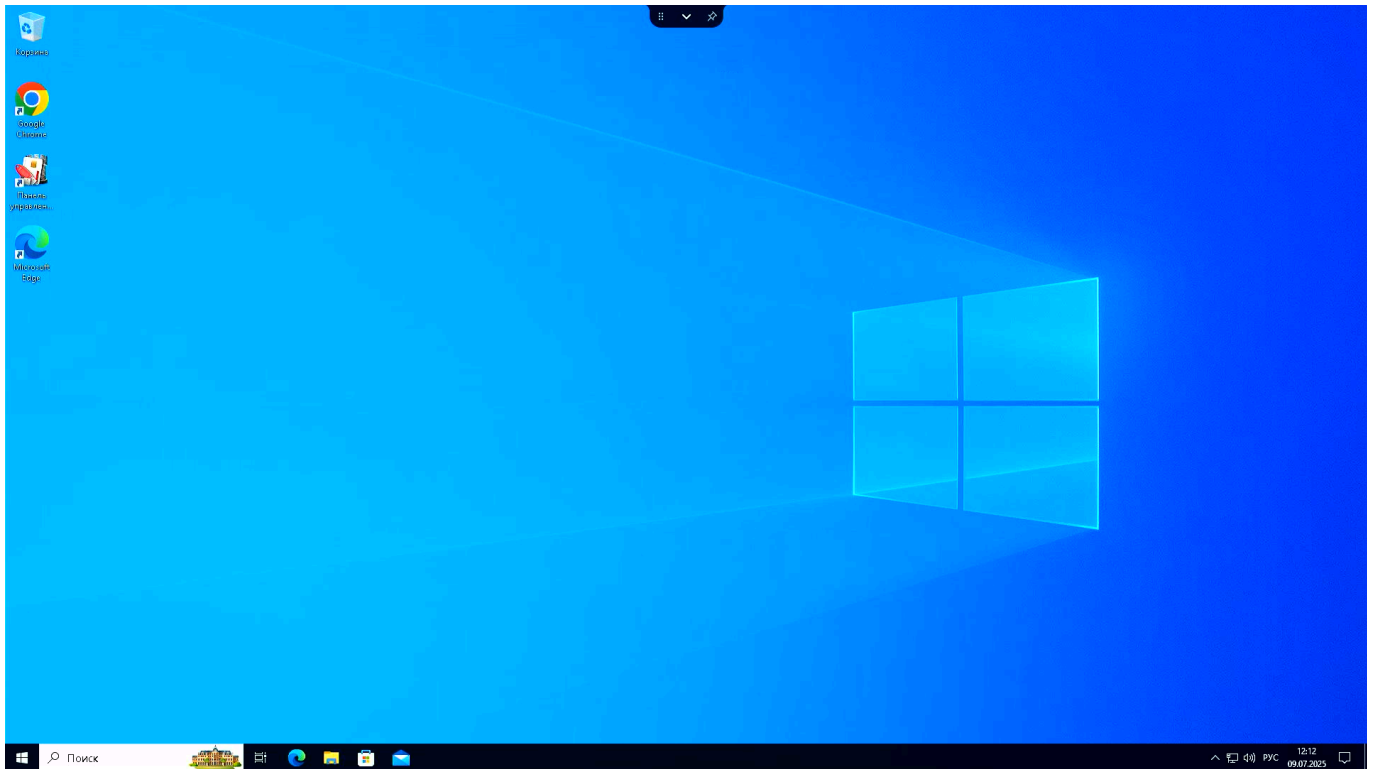
- Hidden.

The panel is not displayed on the screen.

If the connection panel is not pinned, it collapses automatically when out of keyboard or mouse focus.

- Collapsed.

The connection panel control elements are displayed when you hover the cursor over the upper part of the screen (see the figure below).



Window showing a running remote session with the collapsed connection panel

Changing the connection panel state

In the Kaspersky Thin Client interface, you can change the state of the connection panel and also move the collapsed panel horizontally and pin it anywhere on the screen.

You can change the connection panel state as follows:

- If you want to completely hide the expanded connection panel, do one of the following:
 - press **CTRL+ALT+HOME** or **ESC**
 - click on any area of the screen outside the panel
- If you want to display a collapsed connection panel, hover the cursor over the top of the screen. The panel control elements are displayed.
- If you want to expand the connection panel, do one of the following:
 - press **CTRL+ALT+HOME**
 - restore the collapsed connection panel and click the  button

You can manage a minimized connection panel in the following ways:

- If you want to change the position of the panel, click and hold the  button and move the panel to the right or left.
- If you want to pin a collapsed panel in its current position, click the  button.
The connection panel will be displayed in its collapsed state at the top of the screen until you hide or unpin it.
- If you need to unpin the panel, click the  button.

The position of the collapsed panel on the screen is saved for future connections, even after the thin client is restarted or shut down.

Locking and unlocking a remote session

Kaspersky Thin Client automatically locks remote sessions when the screen goes dark after a period of idle time [specified in the thin client's settings](#). You can also lock and then unlock a remote session manually.

To lock a running remote session,

either press **Win+L** or [expand the connection panel](#) and click .

The remote session will be locked. A lock screen will be displayed.

To close a locked remote session:

1. Move the mouse or press any key.
2. On the screen that appears, click **Terminate the remote session**.

The remote session will be closed, and the application window in which you started the remote session will be displayed.

To unlock a remote session:

1. Move the mouse or press any key.
2. On the screen that appears, type the password you used to connect to the remote system.
If you initially authenticated with a [broker](#) or another remote connection service, you need to enter the same password you used to connect to that service.
3. Click **Unlock**.

The remote session will be unlocked. The remote environment screen will be displayed.

Closing a remote session

To close a remote session,

[restore the connection panel](#) and click  or press **CTRL+D**.

The remote session will close, and a connection window will be displayed.

Managing audio playback and recording devices in the connection panel

You can connect several audio playback and recording devices to a thin client running Kaspersky Thin Client via a mini-jack or USB port to redirect these to the remote environment. In the Kaspersky Thin Client interface, you can [switch between connected devices](#).

Audio volume and other settings are managed from the remote environment.

When connecting to a remote environment deployed in the Citrix Workspace infrastructure, redirection of more than two USB devices simultaneously is not supported.

Connection via mini-jack is not supported on Dell Wyse 3040 thin clients.

To select audio playback and recording devices in a remote session:

1. [Restore the connection panel](#) and click the  button in the opened panel.
2. In the opened window, select the audio playback device from the **Output** list and select the audio recording device from the **Input** list.

If the device you want to use does not appear in the list, check the redirection settings in the application that you used to connect to the remote environment, or contact your company administrator.

Managing virtual application windows

When connecting to a [virtual application](#), you can switch between its windows in the Kaspersky Thin Client connection panel.

To switch to another window of a running virtual application:

1. Restore the connection panel.
2. Click the application icon.
A list of open application windows is displayed.
3. Click the relevant window.

The selected virtual application window is displayed.

Web Access: redirecting USB devices to a remote environment

You can redirect printers, scanners, webcams, and USB drives to a remote environment deployed in a Citrix Workspace infrastructure. Webcam redirection does not require additional configuration in the remote environment.

No more than two [USB devices](#) can be redirected at the same time.

Redirecting a printer or scanner to a remote environment

To redirect a printer or scanner to a remote environment:

1. Connect the device to the thin client via the USB connector.
2. If you are connecting a scanner, [manually specify the device type](#) under **Settings** -> **Unrecognized USB devices**.
3. [Connect to a remote environment in the Web Access application](#).
4. Expand the Citrix Workspace control panel at the top of the window and click the **USB Devices** button.
You will see a window prompting you to redirect the USB device.
5. Click **Add**.
You will see a window showing a list of devices available for redirection.
6. If the relevant device does not appear in the list, try restarting the remote session without removing the USB device.
7. Select the relevant device in the list and click **Connect**.

The device will be redirected to the remote environment. You can now use it in a remote desktop.

If you need to redirect multiple devices, repeat steps 4–6 of these instructions for each of them.

For more information about redirection of USB devices, please refer to the [Citrix Workspace product documentation](#).

Redirecting USB devices to a remote environment

You can also redirect USB drives to the remote environment and then safely remove them. Redirection uses Client Drive Mapping technology. For more details, please refer to the [Citrix Workspace product documentation](#).

To redirect USB drives to a remote environment deployed in a Citrix Workspace infrastructure:

1. Connect the device to the thin client via the USB connector.
2. [Connect to a remote environment in the Web Access application](#).
3. Expand the Citrix Workspace control panel at the top of the window and click **Map a drive**.
You will see the window for selecting the mount directory.

4. Click **Browse**.

A confirmation window is displayed.

5. Click **Redirect** to confirm the redirection of all USB drives connected to the thin client.
You will see the window for selecting the mount directory.

6. Click **Add** to confirm the redirection.

7. Terminate the remote session and connect to the remote environment again to complete the redirection.

The USB drives will be redirected to the remote environment. A disk containing folders with the names of the redirected USB drives will be displayed in the file system of the remote environment.

Safely ejecting USB devices in a remote session

Kaspersky Thin Client supports safe removal of USB drives in a remote session. To avoid damage to the data stored on the device, eject the device according to the instructions below.

To safely eject a USB drive in a remote session:

1. [Connect to a remote environment in the Web Access application](#).
2. [Restore the connection panel](#) and click the  button.

You will see a list of USB devices that have been redirected to the remote environment.

3. Select the relevant device or click **Eject all USB drives**.
4. If there is a problem encountered with safe removal, an error message is displayed. Close all windows on the remote desktop and terminate the copying processes, then try again.

The device is now ready to be safely removed and you can physically disconnect it from the thin client.

Viewing information about Kaspersky Thin Client and a thin client

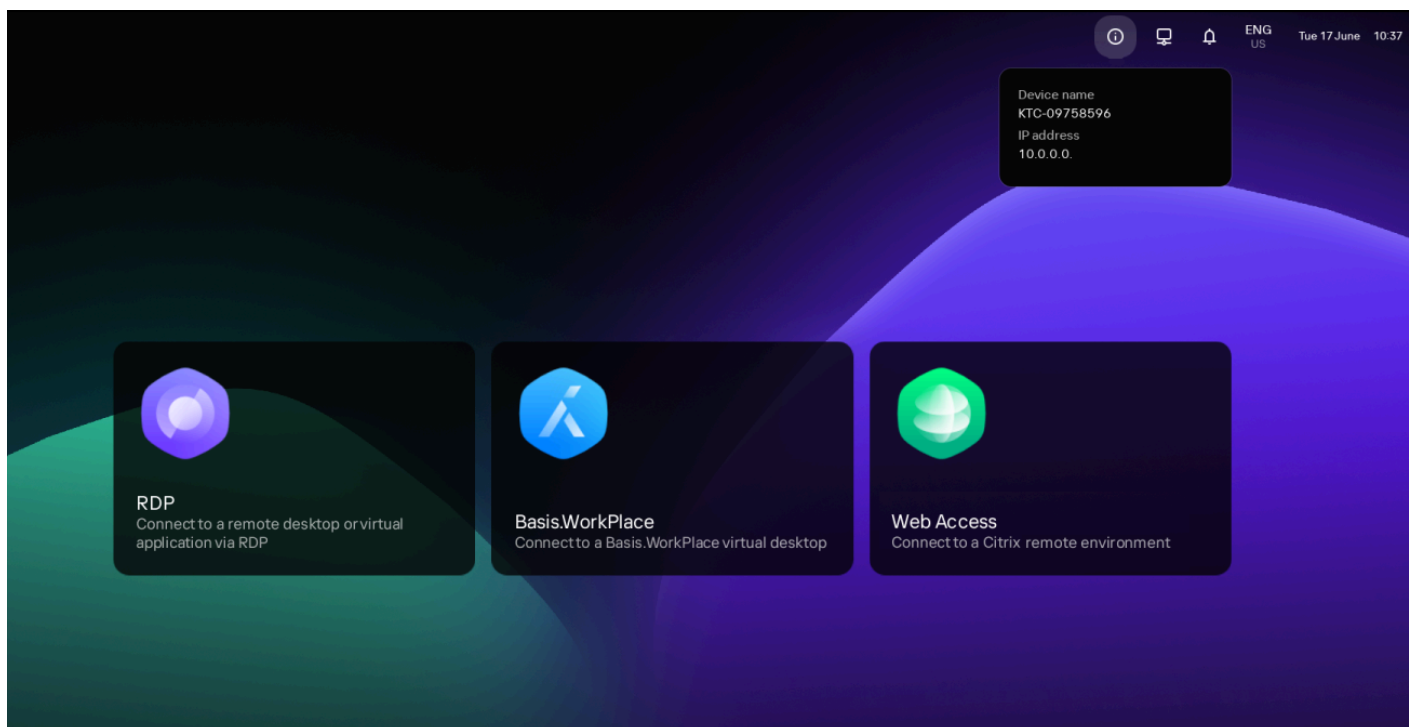
In the Kaspersky Thin Client interface, you can view the current version of the operating system and its release date, and the SDK version. The interface also displays the IP address and name of the thin client.

To view information about a thin client,

in the Kaspersky Thin Client control panel, click .

A window containing information about the thin client appears.

This window will also display the Technical Support contacts or your company's administrator contacts if the thin client was added to the [administration group](#) and if this data was [specified in the policy via the Web Console](#).

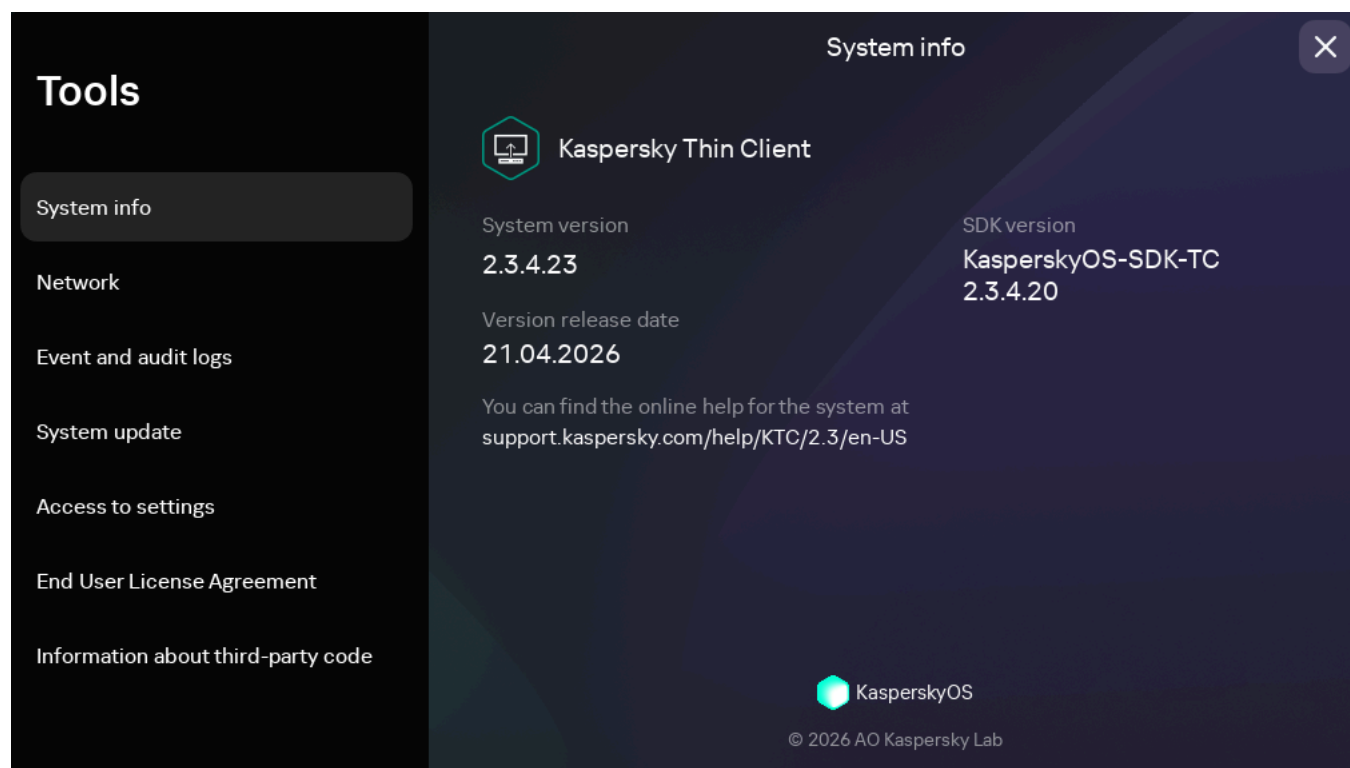


Thin client information window

To view information about Kaspersky Thin Client,

in the Kaspersky Thin Client control panel, click  and select **Tools** → **System info** in the menu that opens (see the figure below).

A window with information about Kaspersky Thin Client will appear.



Tools. System info section

Viewing network status information

In the Kaspersky Thin Client interface, you can view the settings for connecting the system to the network and view information regarding the network connection status. Information about Kaspersky Thin Client network connection settings is updated automatically at least once every second.

To view information about the network connection status,

in the Kaspersky Thin Client control panel, hover over the icon .

A window containing information about the status of the network connection will appear.

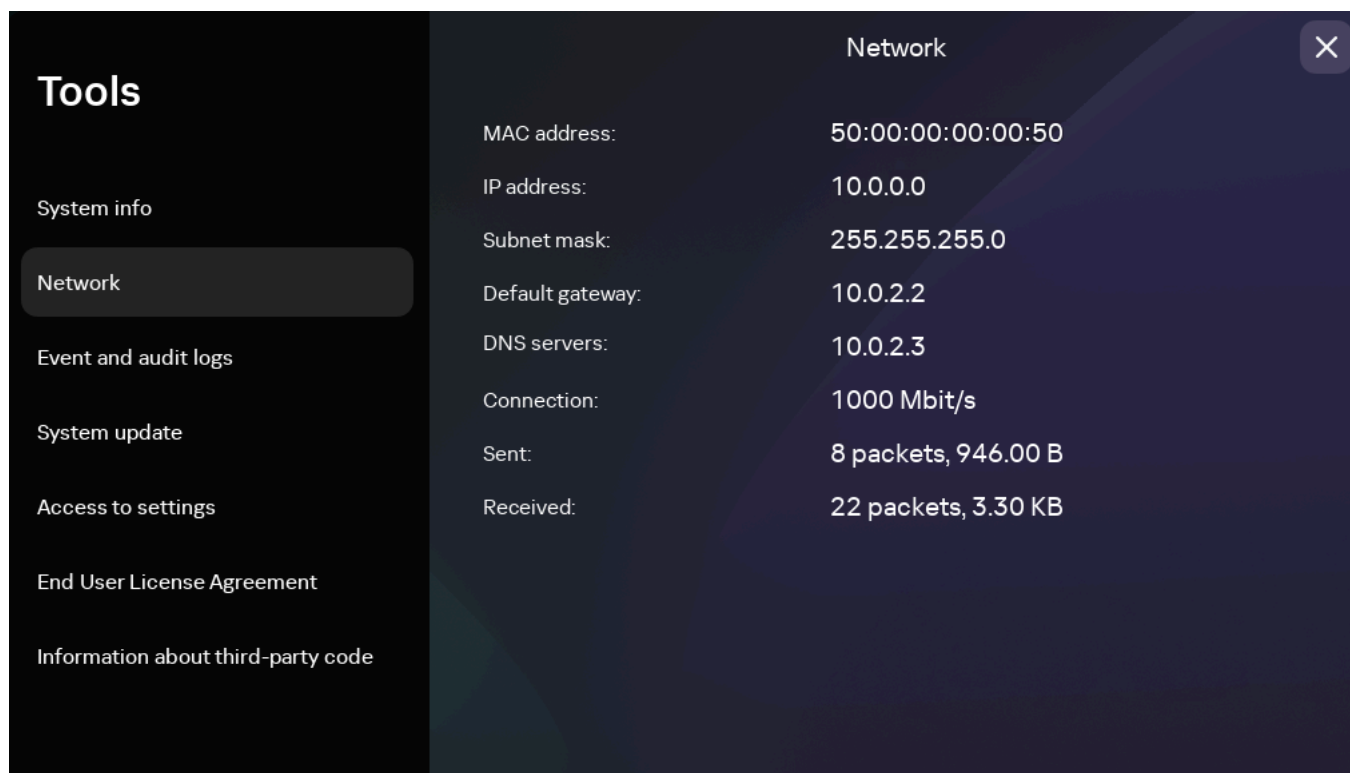
To view the network connection settings,

in the Kaspersky Thin Client control panel, click  and select **Tools** → **Network** in the menu that opens (see the figure below).

A window showing the settings for connecting Kaspersky Thin Client to the network will appear (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.



Tools. Network section

Viewing Kaspersky Thin Client notifications

The Kaspersky Thin Client interface displays the following types of notifications:

- Prompts to select an action by clicking a button, for example, run or defer an update. After some time, Kaspersky Thin Client will repeat any prompts that you closed without selecting an action. A prompt is considered to be resolved after you select an action.
- Prompts to go to another section of Kaspersky Thin Client to configure further settings. For example, the system prompts the user to set up monitor layout when you connect a second monitor. You can choose between going to the other system section by clicking the appropriate button or dismissing the prompt.
- Informational notifications. These notifications do not require you to take any action. Your only option is to close the notification after reviewing its contents.

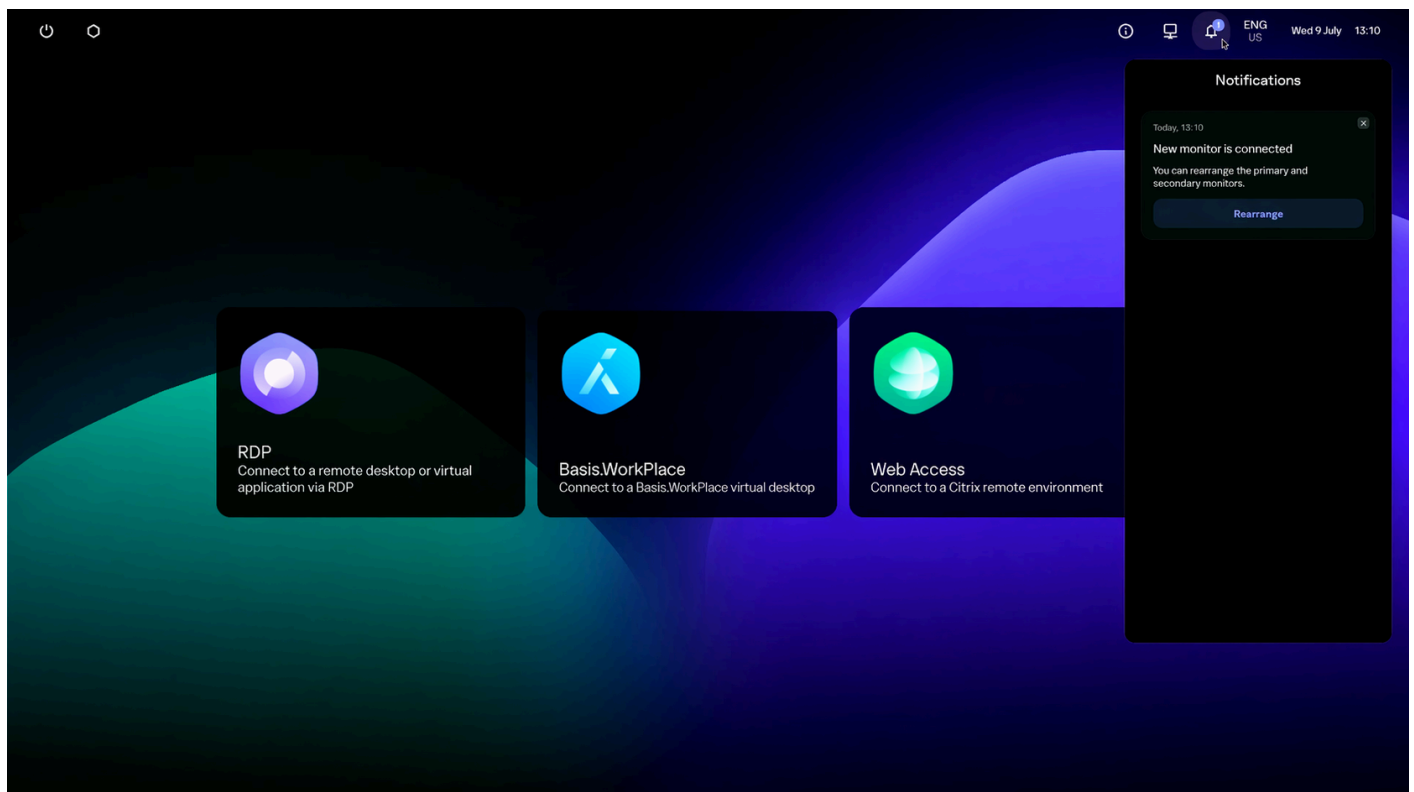
If the cursor or keyboard focus are outside the notification area, unresolved and unread prompts are hidden, and the counter in the control panel displays their number.

Update notifications are not hidden automatically in remote sessions. You will need to dismiss them manually or perform the required action to make them go away.

To view a list of all Kaspersky Thin Client notifications,

in the Kaspersky Thin Client [control panel](#), click .

The notifications panel will appear. If you have new notifications, they will be displayed in the panel (see the figure below).



Kaspersky Thin Client notifications panel

Managing certificates in the Kaspersky Thin Client interface

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

About certificates for connecting to Kaspersky Security Center

If the Kaspersky Security Center administrator replaces the [certificate for connecting to Kaspersky Security Center](#), some cases may require confirmation of the certificate replacement. 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 mobile certificate for connecting to Kaspersky Security Center:

1. Turn on Kaspersky Thin Client.
2. In the **Certificate must be replaced** 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 must be replaced** 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.

About certificates used to connect to a remote environment and to a log server

If a thin client is not connected to Kaspersky Security Center and the administrator has not assigned certificates for it in the Web Console, a user could also connect to nodes and use certificates that are not controlled by the administrator. We recommend configuring the [connection of an administration group](#) to a log server and to a remote environment only by using certificates that were assigned by the administrator in the Web Console. These measures will help prevent Kaspersky Thin Client from connecting to untrusted nodes.

You can use or reject a certificate in the Kaspersky Thin Client interface in the following cases:

- [when connecting Kaspersky Thin Client to Kaspersky Security Center for the first time](#)
- when connecting to a remote environment for the first time
- [when connecting to a log server for the first time](#)

Accepted certificates are saved in the system store of Kaspersky Thin Client.

If a thin client is included in an [administration group](#) and this group has been [assigned certificates in the Web Console](#), you will not be able to manage the certificates in the Kaspersky Thin Client interface.

Managing Kaspersky Thin Client using hotkeys

You can use dedicated keyboard shortcuts while working with Kaspersky Thin Client and during [remote sessions](#). The table below lists all the available hotkeys and key combinations.

Keys and key combinations	Actions
Win	Open or close the shut down menu .
→ ←	Switch between applications (RDP, Basis.WorkPlace, Web Access) on the Kaspersky Thin Client desktop .
↑ ↓	- Switch between drop-down list items. - Scroll page content up or down.
Tab	Switch <i>left to right</i> or <i>top to bottom</i> between the following: - Connection options. - The order of fields, for example, in the Settings window. - Buttons in the connection panel. When switching, unavailable items, such as disabled fields, and inactive items are skipped.
Shift+Tab	Switch <i>right to left</i> or <i>bottom to top</i> between the following: - Connection options. - The order of fields, for example, in the Settings window. - Buttons in the connection panel. When switching, unavailable items, such as disabled fields, and inactive items are skipped.
Space or Enter	- Click the button with keyboard focus on it. - Open or close the drop-down list with keyboard focus on it. When switching, unavailable items, such as disabled fields, and inactive items are skipped.
Esc	- Close the active window. - Collapse the connection panel with keyboard focus on it.
Alt+Shift	Change the keyboard language.
Alt+Page down Alt+Page up	Navigate to the next or previous section of 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 .
Ctrl+D	Close the remote session. The shortcut only works on an expanded connection panel.
Win+I	Open Settings from the Kaspersky Thin Client desktop if access to the settings is unblocked .
Win+U	Open Tools from the Kaspersky Thin Client desktop.
Win+L	Lock a running remote session.
Win+Esc	Shut down Kaspersky Thin Client from the Kaspersky Thin Client desktop.
Win+F12 or Win+End	Restart Kaspersky Thin Client from the Kaspersky Thin Client desktop.
Win+A or Win+N	Open the notifications panel from the Kaspersky Thin Client desktop.
Win+↓ Win+↑	Collapse or restore a window while you are connected to a virtual application.
Win+M	Minimize all windows while you are connected to a virtual application.
Win+Shift+M	Restore all windows while you are connected to a virtual application.

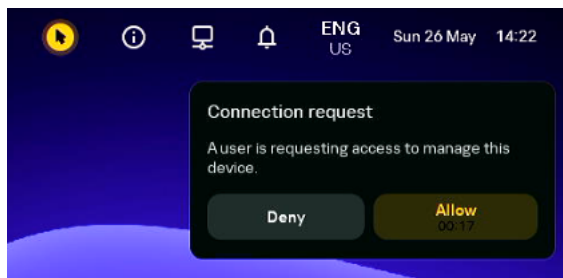
Managing access to remote management and to the remote environment screen

In Kaspersky Thin Client, you can accept and reject requests for access to remote management of the thin client and for access to the screen of the [remote session](#) (hereinafter also referred to as the "remote environment screen").

To accept or decline a request for access to remote device management and to the remote environment screen:

1. [Turn on the thin client](#) and make sure that the [device is connected to the network](#).

When you try to connect to Kaspersky Thin Client, the  icon is displayed in the control panel. A notification requesting connection will appear on the desktop (see the figure below).



The Kaspersky Thin Client desktop notification containing a request to remotely manage the thin client

2. Do one of the following:

- Click **Deny** to prevent remote management access to Kaspersky Thin Client.
- Click **Allow** to allow the administrator to view the Kaspersky Thin Client screen and manage system settings.

Accept the request only if you are sure that your company administrator is the person connecting to Kaspersky Thin Client.

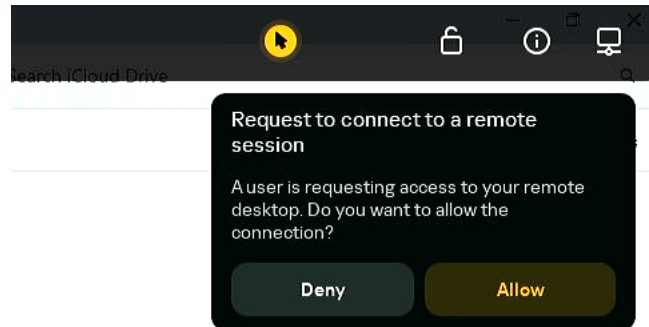
Management of Kaspersky Thin Client will be transferred to the administrator.

If the **Allow automatically** mode is configured [for a device](#) or [its administration group](#) in the [Kaspersky Thin Client settings](#) or in the remote management settings in the Web Console and there is no response to the request within 30 seconds, management of the Kaspersky Thin Client is automatically transferred to the administrator.

3. If a [remote session](#) is running in Kaspersky Thin Client at the time of the remote connection or if a remote session is started by the administrator during remote management of the device, access to the screen of such a remote session is regulated as follows:

- If automatic connection to the remote screen is allowed [for the device](#) or [its administration group](#) in the [Kaspersky Thin Client settings](#) or in the remote management settings in the Web Console, the administrator is automatically granted access to the screen of the running remote session.
- If the mode of access to the remote environment screen is set to **Allow by request** in the Kaspersky Thin Client settings or in the remote management settings in the Web Console, a notification containing a request to connect to the remote session is displayed in the Kaspersky Thin Client interface (see the figure below).

Management of Kaspersky Thin Client will be automatically transferred to the user.



Notification containing a remote session connection request

4. Do one of the following:

- Click **Deny** to prevent administrator access to the remote environment screen.
If you want to transfer thin client management to the administrator again but without giving them access to the remote environment screen, [terminate the remote session](#).
- Click **Allow** to allow the administrator to view the remote environment screen and manage the remote session.

Management of Kaspersky Thin Client will be transferred to the administrator.

Remote connection to a thin client

An administrator can remotely connect to a thin client from their device for the purpose of remotely managing the thin client by using an RDP client to resolve problems or help the user configure Kaspersky Thin Client.

For remote management to work, the thin client must be [On](#) and [connected to the network](#). Either the **Allow automatically** or **Allow by request** remote management access mode must be set for the [thin client](#) or [its administration group](#) in the [Kaspersky Thin Client settings](#) or in the remote management settings in the Web Console.

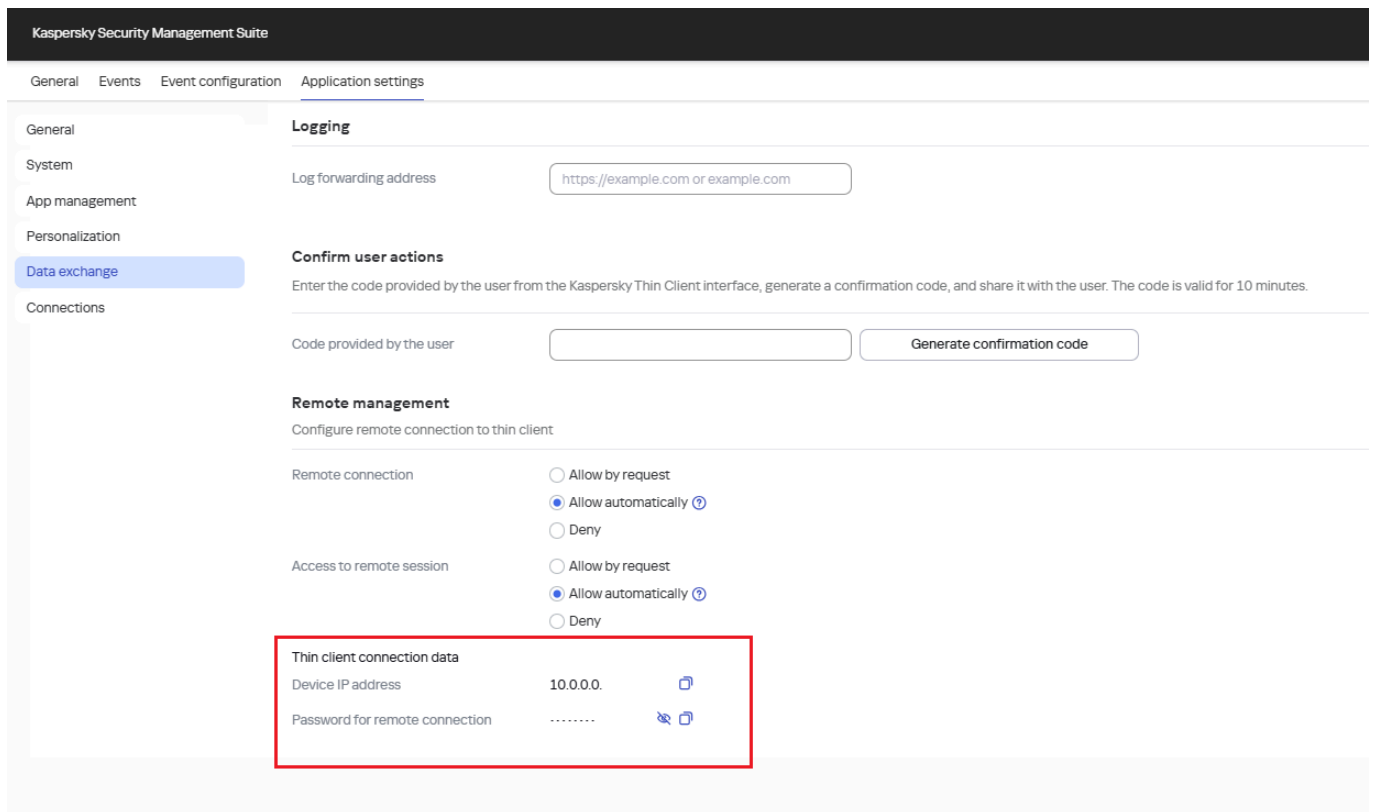
The thin client's IP address and remote connection password (hereinafter also referred to as "credentials") are necessary for a remote management.

To connect to a thin client for remote management purposes:

1. Open the RDP client on the device from which you will connect to the thin client.
2. Obtain the remote connection credentials in one of the following ways:
 - If the thin client is [connected to Kaspersky Security Center](#), copy the credentials in the Web Console interface:
 - a. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices** if you want to connect to a device from an administration group, or select **Discovery & deployment** → **Unassigned devices** if you want to connect to a device that is not part of any administration group.
 - b. In the opened list, click the [name of the thin client](#) that you want to connect to.
 - c. In the window that opens, select the **Applications** tab.
 - d. Click the name of the Kaspersky Security Management Suite web plug-in.
 - e. In the window that opens, select the **Application settings** tab.
 - f. Go to the **Data exchange** section.

g. In the **Thin client connection data** block, copy the remote connection account credentials by clicking the  button next to them (see the figure below).

The password for remote connection in the Web Console is updated once a day and after each restart of the thin client.



The screenshot shows the 'Kaspersky Security Management Suite' interface. On the left is a sidebar with navigation links: General, Events, Event configuration, Application settings, General, System, App management, Personalization, Data exchange (highlighted), and Connections. The main area is titled 'Logging' and contains sections for 'Confirm user actions' and 'Remote management'. The 'Remote management' section is titled 'Configure remote connection to thin client' and includes radio button options for 'Remote connection' and 'Access to remote session'. At the bottom, a 'Thin client connection data' block is highlighted with a red rectangle. It contains two rows: 'Device IP address' with the value '10.0.0.0' and a copy icon, and 'Password for remote connection' with a masked password '.....' and both copy and refresh icons.

Configuration window for remote management of a thin client in the Web Console

- If the thin client is not connected to Kaspersky Security Center, request the default password from [Technical Support](#) and [get the device's IP address in the Kaspersky Thin Client interface](#).

The default password is intended for temporary use. Use it only if the thin client is not yet connected to Kaspersky Security Center.

3. In the RDP client installed on your device, enter the received credentials and start connecting to the thin client.
4. To connect to the thin client, depending on the specific remote management access mode that is configured in the [Kaspersky Thin Client settings](#) or in the remote management settings in the Web Console [for the device](#) or its [administration group](#), do one of the following:
 - If the **Allow automatically** mode is set, wait until the connection to the thin client is established.
The user can accept or reject your request within 30 seconds. If the user does not take any action during this time, the connection starts automatically.
 - If the **Allow by request** mode is set, wait until the user [accepts the remote management request in the Kaspersky Thin Client interface](#).

If you've successfully connected to the thin client, the remote environment screen access window is displayed.

5. To gain access to the remote environment screen, depending on the mode that is configured in the [Kaspersky Thin Client settings](#) or in the remote management settings in the Web Console [for the device](#) or its [administration group](#), do one of the following:

- If the **Allow automatically** mode is set, wait until the connection to the thin client is established.
- If the **Allow by request** mode is set, wait until the user accepts the connection request in the Kaspersky Thin Client interface or [terminates the remote session](#).
- If the mode is set to **Deny**, wait until the user terminates the remote session.

The Kaspersky Thin Client interface is displayed. You will gain access to the Kaspersky Thin Client remote management.

To terminate remote management of the thin client in the Kaspersky Thin Client interface,

in the [connection panel](#), click the  button. In the opened window, click **Terminate**.

Managing Kaspersky Thin Client via the Kaspersky Security Center Web Console

The Kaspersky Security Center Web Console (hereinafter also referred to as simply "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 Online Help](#).

Kaspersky Thin Client 2.3 supports Kaspersky Security Center Linux version 15.3 and Kaspersky Security Center Web Console version 15.3.

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 via the Kaspersky Security Center Web Console.

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

- manage Kaspersky Thin Client settings [for one](#) or [more thin clients](#) in an [administration group](#)
- [configure receipt of Kaspersky Thin Client events and view them](#)
- [manage security certificates of Kaspersky Thin Client](#)

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

- [specify the Kaspersky Security Center connection settings](#) when configuring Kaspersky Thin Client
- [install the Kaspersky Security Management Suite web plug-in](#) in Kaspersky Security Center

To ensure stable operation of system functions and access to all of its capabilities, the major versions of the web plug-in of Kaspersky Security Management Suite and Kaspersky Thin Client must match.

Installing the Kaspersky Security Management Suite web plug-in

Kaspersky Security Management Suite, 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.

You can view the list of installed web plug-ins in the Web Console interface (**Console settings** → **Web plug-ins**).

The web plug-in functionality is available to all administrators with browser access to the Web Console. If required, you can [set up access control for the 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 more information about enabling a port on the Kaspersky Security Center Administration Server, see the [Kaspersky Security Center Online Help](#).

To ensure stable operation of system functions and access to all of its capabilities, the major versions of the web plug-in of Kaspersky Security Management Suite and Kaspersky Thin Client must match.

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

1. Open the relevant archive containing web plug-in installation images and signature files included in the [Kaspersky Thin Client distribution kit](#).

The End User License Agreement is displayed.

2. Read the End User License Agreement and accept it if you agree with the terms therein.

The relevant archive containing web plug-in installation images and signature files is unpacked automatically after you accept the agreement.

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

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

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

5. In the panel that opens, add the files from the unpacked archive containing web plug-in installation images and signature files:

- ZIP archive containing the plug-in distribution package (`plugin.zip`), by clicking **Upload ZIP file**;
- signature file (`signature.txt`), by clicking **Upload signature**.

6. Click the **Add** button.

7. 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 appear in the list of Web Console management plug-ins.

Updating the Kaspersky Security Management Suite web plug-in

To update Kaspersky Security Management Suite, obtain an archive containing the web plug-in installation package and an archive digital signature from Kaspersky.

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

1. Open the archive containing the web plug-in installation images and signature files that you received from Kaspersky.
The End User License Agreement is displayed.
2. Read the End User License Agreement and accept it if you agree with the terms therein.
The relevant archive containing web plug-in installation images and signature files is unpacked automatically after you accept the agreement.
3. In the Web Console menu, select **Console settings** → **Web plug-ins**.
4. In the displayed list of Web Console plug-ins, find Kaspersky Security Management Suite and click it.
5. In the window that opens, click the **Update from file** button.
6. In the panel that opens, add the files from the unpacked archive containing web plug-in installation images and signature files:
 - ZIP archive containing the plug-in distribution package (`plugin.zip`), by clicking **Upload ZIP file**;
 - signature file (`signature.txt`), by clicking **Upload signature**.
7. Click **Update**.
8. 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 via the Web Console interface.

Prior to removing the web plug-in, delete the managed devices from [administration groups](#).

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

1. In the Web Console menu, select **Console settings** → **Web plug-ins**.
A list of available Web Console plug-ins is displayed.
2. In the list of 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, refer to the [Kaspersky Security Center Online Help](#).

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

- *Security Officer*. Only [certificate management](#) is allowed for this role. You can assign this role to an employee in charge of the information security in your enterprise.
- *Administrator*. This role is granted access to all management functions of Kaspersky Thin Client via the Web Console except for certificate management.
- *Advanced administrator*. This role is granted access to all management functions of Kaspersky Thin Client via the Web Console. 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 lists the Kaspersky Thin Client management functions that are available to the user depending on their assigned role. 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 a remote environment in a Kaspersky Security Management Suite policy	–	✓	✓
Configuring general settings in a Kaspersky Security Management Suite policy	–	✓	✓

Function	Security Officer	Administrator	Advanced administrator
Managing system settings in a Kaspersky Security Management Suite policy	–	✓	✓
Managing Kaspersky Thin Client data in a Kaspersky Security Management Suite policy	–	✓	✓
Managing Kaspersky Thin Client applications in a Kaspersky Security Management Suite policy	–	✓	✓
Configuring personalization settings in a Kaspersky Security Management Suite policy	–	✓	✓

Logging in and out of the Web Console

To log in to the Web Console, you will need the Kaspersky Security Center Administration Server web address and port number that were specified during installation (port 8080 is used by default). You must also enable JavaScript in your browser. For the Kaspersky Security Center Web Console browser requirements, please refer to the [Hardware and software requirements](#) section of the Kaspersky Security Center Online Help.

To log in to the Web Console:

1. In your browser, go to `https://<Administration Server address>:<Port number>`.

The login page opens.

2. Log in using the domain user name and password.

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. You can navigate through the Web Console and use it to work with Kaspersky Security Center.

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.

Managing policies and administration groups

In the Web Console, you can add thin clients running Kaspersky Thin Client and connected to Kaspersky Security Center to an [administration group](#) to [configure system settings](#) using [policies](#) in a centralized manner.

By default, immediately after installing Kaspersky Security Center, there is one group in the hierarchy of administration groups—**Managed devices**. Any groups you create will be its child groups. In the policy created for the **Managed devices** group, you can configure devices across all administration groups. For example, we recommend using the policy to [add certificates](#) in a centralized manner. For more information about the hierarchy of groups and policies, see the [Kaspersky Security Center Online Help](#).

This section provides instructions on creating administration groups, adding thin clients to them, as well as creating and editing policies. For more information, please see the [policy](#) and [device management](#) sections in the Kaspersky Security Center Help.

Creating an administration group

In the Web Console, you can create [administration groups](#) and add thin clients running Kaspersky Thin Client and connected to Kaspersky Security Center to these groups to [configure device settings](#) using [policies](#) in a centralized manner.

To create an administration group:

1. In the main Web Console window, go to **Assets (Devices) → Hierarchy of groups**.
2. Select the check box next to the administration group that the new group should be a part of.
If you haven't created any administration groups yet, select the **Managed devices** group.
3. Click the **Add** button.
4. In the panel that opens, type in a new administration group name and click **Add**.

The name of an administration group must be unique within its hierarchy.

The new group will appear in the list of administration groups.

Adding thin clients to the administration group

You can add thin clients running Kaspersky Thin Client to the [administration group you created](#) or to the **Managed devices** group.

To add devices to the administration group:

1. In the main window of the Web Console, select **Discovery & deployment → Unassigned devices**.
A list of all devices connected to Kaspersky Security Center but not added to any administration group will be displayed.
2. Select the check boxes next to the devices you want to add to the group.
3. Click the **Move** button.
4. In the panel that appears, select the administration group.
5. Click the **Move** button.

The devices will be added to the selected administration group.

You can also automate the process of moving thin clients into administration groups. For more details, please refer to the [Kaspersky Security Center Online Help](#).

Policy creation

To configure Kaspersky Thin Client installed on thin clients from an [administration group](#), create a [policy](#) for that group in the Web Console.

By default, immediately after installing Kaspersky Security Center, there is one group in the hierarchy of administration groups—**Managed devices**. Any groups you create will be its child groups. In the policy created for the **Managed devices** group, you can configure devices across all administration groups. For example, we recommend using the policy to [add certificates](#) in a centralized manner. For more information about the hierarchy of groups and policies, see the [Kaspersky Security Center Online Help](#).

To create a policy:

1. In the main window of the Web Console, select **Assets (Devices) → Policies & profiles**.
2. Select the required administration group. To do this, click the current path at the top of the window and, in the panel that opens, click the required administration group.
3. Click the **Add** button.
4. In the list of applications displayed in the opened window, select the Kaspersky Thin Client administration web plug-in and click **Next**.
5. In the new policy configuration window, on the **General** tab, specify the following settings:
 - In the **Name** field, enter the policy name.
 - In the **Policy status** block, select one of the following statuses:
 - **Active**

The policy that is currently applied to devices in the administration group. If this option is selected, the next time you synchronize Kaspersky Thin Client and Kaspersky Security Center, this policy will become active. Each administration group can have only one active policy.

This status is selected by default.
 - **Inactive**

The policy that is not currently applied to devices in the administration group. If this option is selected, the policy becomes inactive but remains in the list of policies. You can later activate an inactive policy.
 - **Out-of-office**

The policy is activated when the device leaves the organization's network perimeter.
 - Turn on or off the toggles in the **Settings inheritance** block:
 - **Inherit settings from parent policy**

If the toggle is enabled, the policy settings are inherited from the policy for the top-level group and cannot be modified.

By default, the option is enabled.

- **Force inheritance of settings in child policies**

The policy settings will be propagated to the policies of nested administration groups (child policies), and in the **Settings Inheritance** block, in the **General** section of each child policy properties window, the **Inherit settings from parent policy** option will be enabled automatically.

When this setting is enabled, the child policy settings cannot be modified.

By default, the option is disabled.

For more information about the hierarchy of groups and policies, see the [Kaspersky Security Center Online Help](#).

6. If you want to [customize other settings](#), select the **Application settings** tab and make the necessary changes.

7. Click **Save** in the lower part of the page.

The policy is created and appears in the list of policies.

Editing a policy

In the Web Console, you can edit a [previously created policy](#).

To change a policy:

1. In the main window of the Web Console, select **Assets (Devices)** → **Policies & profiles**.
2. Select the policy that you need to edit.
3. In the policy configuration window that opens, adjust the [settings as needed](#) on the **General** tab.
4. Click the **Save** button in the lower part of the page.

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

Locking settings in a policy

In each [policy](#), the configurable settings have a lock toggle with a lock icon. The available toggle positions are described in the table below.

Settings block toggle positions

State	Description
 Undefined 	The values assigned to this setting do not apply to devices governed by the policy. The user can change this setting in the Kaspersky Thin Client user interface.
 Enforced 	The values assigned to this setting apply to devices governed by the policy. The user will not be able to change this setting in the Kaspersky Thin Client interface.

Configuring Kaspersky Thin Client settings for one device via the Web Console

In the Web Console, you can configure the settings of Kaspersky Thin Client installed on a thin client. The device must be connected to Kaspersky Security Center and must be [added to an administration group](#).

Changing a thin client ID via the Web Console: one device

In Kaspersky Security Center Web Console, you can change the identifier of a thin client [added to an administration group](#), if a device with the same name already exists in this administration group.

You can configure device names in an administration group [using policies](#).

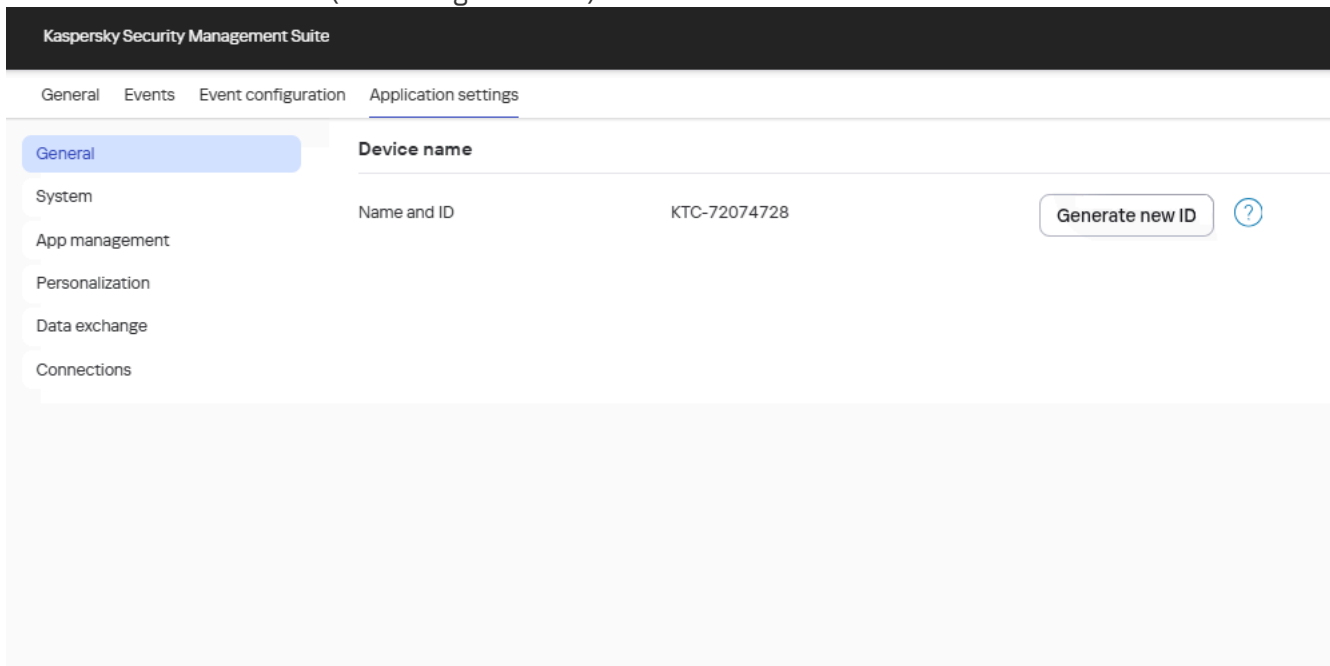
To change a thin client ID via the Web Console:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with information about Kaspersky Thin Client.
5. Select the **Application settings** tab.

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



Changing a thin client ID via the Web Console

7. In the **Device name** group click **Generate new ID**.

This begins the process of creating a new ID. It will be refreshed in the Web Console interface after the thin client synchronizes with Kaspersky Security Center.

8. Click **Save** in the lower part of the window.

The changes are saved and applied to Kaspersky Thin Client installed on a thin client after synchronizing Kaspersky Thin Client and Kaspersky Security Center.

Configuring a connection to a remote environment using the RDP application via the Web Console: one device

In the Web Console, you can configure settings for [connecting to a remote environment using the RDP application](#).

To configure the settings for connecting to a remote environment using the RDP application:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with 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 environment (see the figure below).

The screenshot shows the 'Kaspersky Security Management Suite' web console. The 'Application settings' tab is selected, and within it, the 'RDP' sub-tab is active. The left sidebar shows a navigation menu with 'Connections' highlighted. The main content area is titled 'RDP server settings' and contains the following sections:

- Enter or upload server connection settings:** Includes input fields for 'User name', 'IP address or server name' (with the example '192.168.2.0 or example.com'), and 'Advanced' settings. The 'Advanced' section includes a text area for 'Remote Desktop Connection Broker collection ID' (with the example 'E.g. tsv://MS Terminal Services Plugin.1.coll...'), an input field for 'Application alias (when connected remotely, only the application with this alias opens)', and an 'Upload configuration file' button.
- Auto-connect:** Includes a checkbox for 'Connect automatically' and a red warning icon with text: 'The password that was entered for the last successful connection will be saved and used. You are advised to enable this setting only if unauthorized persons are prevented from accessing the thin client.'
- Connection recovery:** Includes a checkbox for 'Connect again if connection is lost'.

Window for configuring a connection to a remote environment in the RDP application via the Web Console

7. In the **IP address or server name** field, specify the IP address or name of the Microsoft Remote Desktop Connection Broker server.

8. In the **User name** field, enter the name of the user account that will be used for connecting.

9. If you need 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 need to start a virtual application, specify the application alias in the **Application alias** field.

If you have a configuration file containing the settings for connecting to the Microsoft Remote Desktop Connection Broker and, if needed, the name of the application to open, upload the file by clicking **Upload configuration file**. In this case, you do not have to complete the **Remote Desktop Connection Broker collection ID** and **Application alias** fields.

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 **Device redirection** settings block, select the devices to be redirected to the remote environment: **Smart cards, USB drives, Printers and other devices, Microphone, Audio playback devices, Web camera (video), Scanner**.

Audio volume and other settings are managed from the remote environment.

To correctly redirect USB devices to a remote desktop in the Windows 10 operating system, you must enable Microsoft Remote Desktop Services and allow redirection of Plug and Play devices in the settings of Remote Desktop Services. For Microsoft Windows Server 2016 and 2019, you must also enable remote connections via Remote Desktop Services and allow setting remote management rules in Remote Desktop Services.

12. In the **Image quality** block, select the check boxes next to the graphic settings of the remote desktop that you want to use: **Smooth fonts**, **Menu animation**, **Desktop background**, **Show window contents while 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. To improve performance when connected to remote desktops or applications, in the **Performance** block, check **Improve graphics performance**.
15. To automatically connect to a remote desktop or virtual application when the RDP application is started, in the **Auto-connect** block, select the **Connect automatically** check box.

To activate the function, the user must manually connect to and disconnect from the remote environment once. When you do so, the following data for connecting to the RDP server is saved in the thin client storage: user name, server address, and password. The next time you start the RDP application, these credentials will be used to automatically initiate a connection to the remote environment. If you disable the auto-connect function, the saved password is deleted from the device storage.

The Web Console does not let you set a password for connecting to a remote environment.

To automatically connect to the remote environment in the RDP application immediately after booting Kaspersky Thin Client, [configure automatic startup of the application](#).

16. Click **Save** in the lower part of the window.

The changes are saved and applied to Kaspersky Thin Client installed on a thin client after synchronizing Kaspersky Thin Client and Kaspersky Security Center.

Configuring a connection to a remote environment using the Basis.WorkPlace application via the Web Console: one device

In the Web Console application, you can configure the settings for connecting to a remote environment deployed in the Basis.WorkPlace infrastructure.

Users cannot initiate a password change in Kaspersky Thin Client.

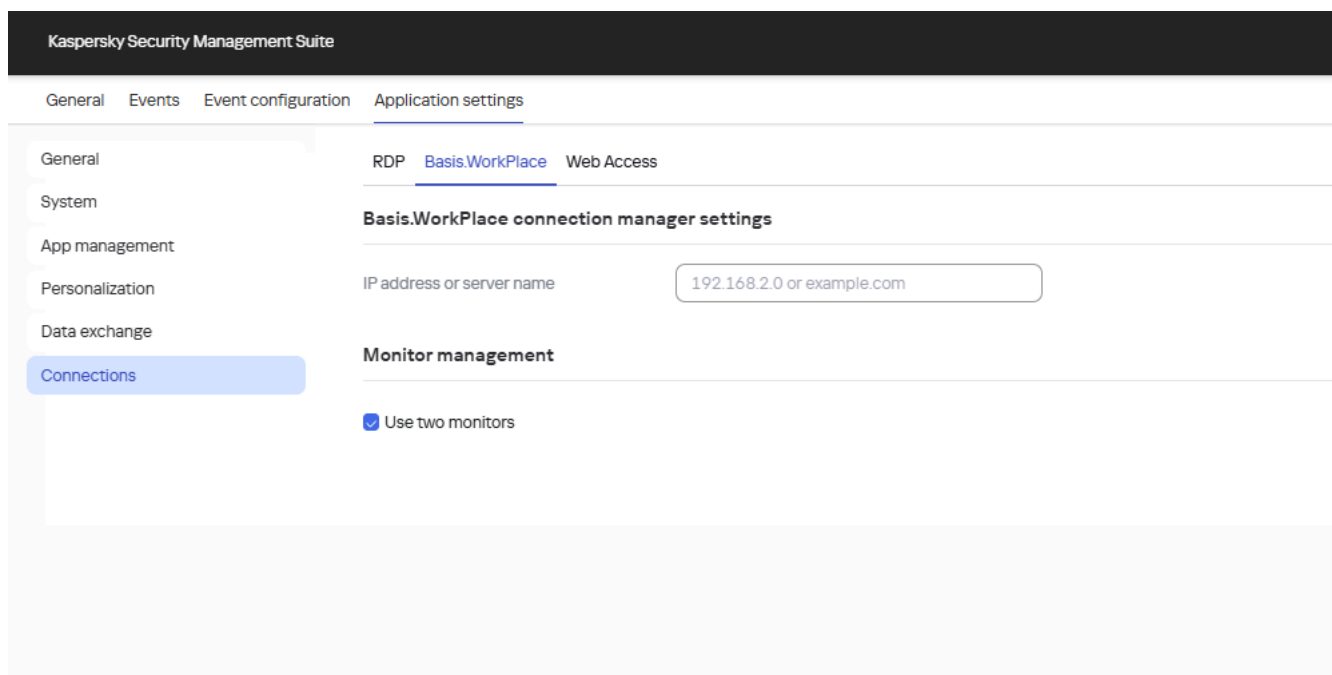
To configure settings for connecting to a remote environment deployed in the Basis.WorkPlace infrastructure:

1. In the main window of the Web Console, select **Assets (Devices) → Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with 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 environment (see the figure below).



Window for configuring settings for connecting to a remote environment deployed in the Basis.WorkPlace via the Web Console

7. In **IP address or server name**, enter the IP address or server name to connect to.
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.

The changes are saved and applied to Kaspersky Thin Client installed on a thin client after synchronizing Kaspersky Thin Client and Kaspersky Security Center.

Configuring a connection to a remote environment using the Web Access application via the Web Console: one device

In the Web Console, you can configure settings for [connecting to a remote environment using the Web Access application](#).

Using the Web Access application, you can connect to a remote environment deployed in the Citrix Workspace infrastructure. Web Access supports HTML5 and provides a secure HTTPS connection when connecting.

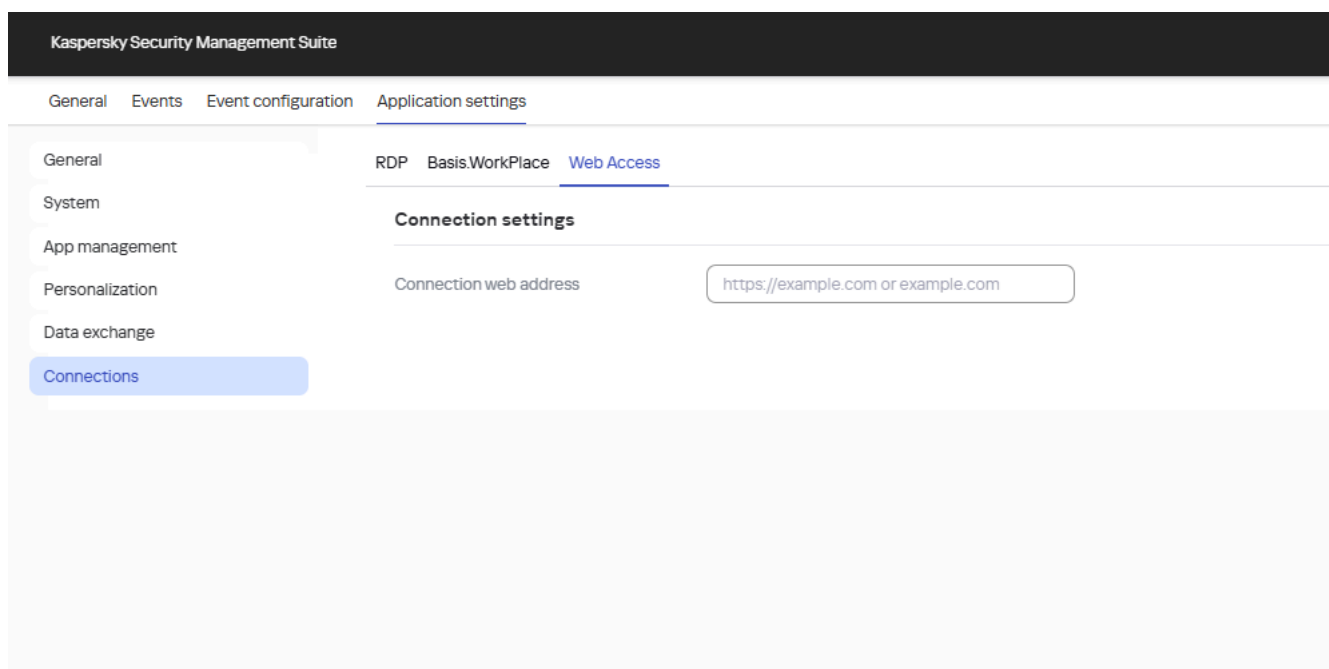
To configure the settings for connecting to a remote environment using the Web Access application:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with information about Kaspersky Thin Client.
5. Select the **Application settings** tab.
6. Select **Connections** → **Web Access**.

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



Configuration window for connecting to a remote environment in Web Access via the Web Console

7. In the **Connection web address** field, enter the server web address for connecting to the [required remote environment](#).

8. Click **Save** in the lower part of the window.

The changes are saved and applied to Kaspersky Thin Client installed on a thin client after synchronizing Kaspersky Thin Client and Kaspersky Security Center.

Configuring monitors and screens via the Web Console: one device

In the Web Console, you can configure monitors connected to a thin client in an [administration group](#) and their screen settings.

Kaspersky Thin Client supports connection of two monitors. The system considers one of the monitors as primary and the other as secondary. During a [remote session](#), the connection panel is displayed on the primary monitor screen. The secondary monitor screen extends or duplicates the image of the primary monitor. In the Web Console, you can select which monitor should be considered the primary monitor (hereinafter also "change the monitor layout").

In the Web Console interface, monitors are numbered. The system determines monitor numbers based on the connection port: monitor 1 is the one nearest to the power source, and monitor 2 is the next one. Refer to the device manufacturer's documentation for the location of the ports on [supported thin client models](#).

The Web Console does not display information about how many monitors are connected to a specific thin client.

If you want the remote session screen to be displayed on both monitors, enable them in the remote environment connection settings in the [RDP](#) or [Basis.WorkPlace](#) applications.

To configure monitors and screens via the Web Console:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with information about Kaspersky Thin Client.
5. Select the **Application settings** tab.

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

Kaspersky Security Management Suite

General Events Event configuration Application settings

General

System

App management

Personalization

Data exchange

Connections

System settings of the device

Interface language English

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

Power-saving settings

Turn off monitor after 5 minutes

Turn off device after 2 hours

Monitor management

If the thin client has two monitors connected to it, the system assigns monitor numbers based on the connection port: Monitor 1 is the one nearest to the power source, and Monitor 2 is the next one.

Primary monitor Monitor 1

Display mode Extend screen

Monitor 1

Monitor resolution 1920×1080

Orientation Landscape

Monitor 2

Monitor resolution 1920×1080

Orientation Landscape

Window for configuring monitors and screens via the Web Console

7. In the **Monitor management** group, configure the required settings:

- In the **Primary monitor** drop-down list, select which monitor should be considered primary.

If only one monitor is connected to the thin client, the settings of the monitor that is set as primary in the Web Console are applied to it.

- In the **Display mode** drop-down list, select the image display option:
 - **Extend screen**—the image spans across two monitors.
 - **Duplicate screen**—the image of the primary monitor's screen is duplicated on the secondary one.
- In the **Monitor resolution** drop-down list, select the desired resolution for the selected screen.

Supported resolutions are listed [in the hardware and software requirements section](#).

If the **Maximum possible** value is selected, the highest value of the parameter supported by the monitor and Kaspersky Thin Client is set.

- In the **Orientation** drop-down list, select the screen position:
 - **Landscape**: the standard screen position.
 - **Landscape flipped**: the screen is rotated 180°.
 - **Portrait**: the screen is rotated 90°.
 - **Portrait flipped**: the screen is rotated 270°.

8. Click **Save** in the lower part of the window.

The changes are saved and applied to Kaspersky Thin Client installed on a thin client after synchronizing Kaspersky Thin Client and Kaspersky Security Center.

Configuring the Kaspersky Thin Client system settings via the Web Console: one device

In the Web Console, you can configure the interface language and time zone of Kaspersky Thin Client, and you can configure the shutdown time for the thin client and monitors connected to it.

Kaspersky Thin Client 2.3 supports the following interface languages: Russian, English (USA), Spanish (Mexico), and Portuguese (Brazil).

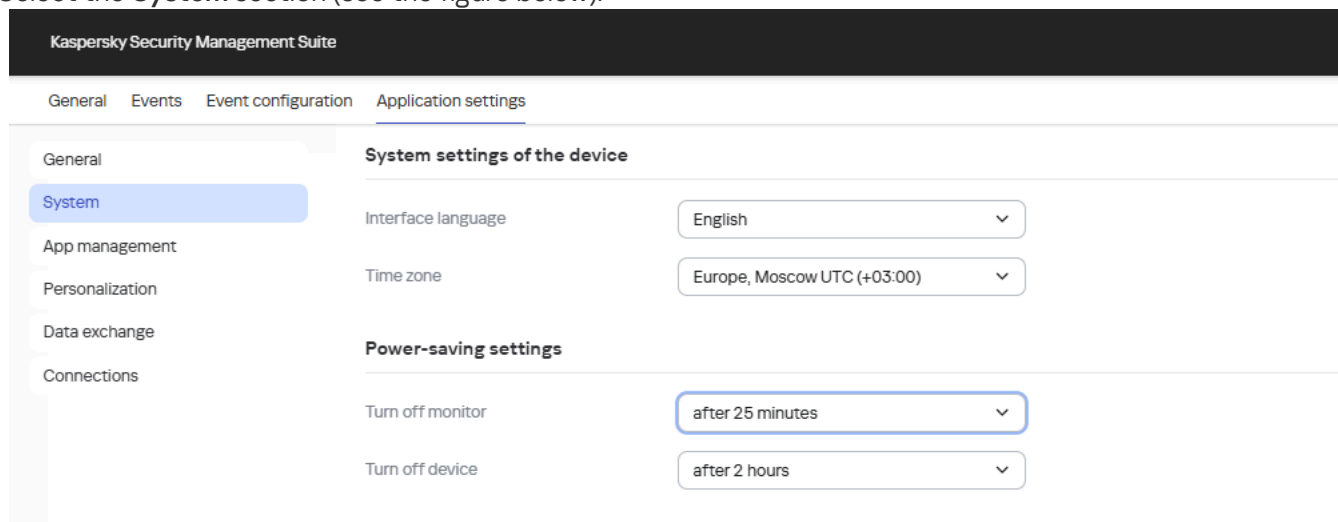
To configure the system settings of Kaspersky Thin Client via the Web Console:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with information about Kaspersky Thin Client.
5. Select the **Application settings** tab.

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



Window for configuring system settings of Kaspersky Thin Client via the Web Console

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

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

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

9. Click **Save** in the lower part of the window.

The changes are saved and applied to Kaspersky Thin Client installed on a thin client after synchronizing Kaspersky Thin Client and Kaspersky Security Center.

Configuring forwarding of Kaspersky Thin Client logs to a log server: one device

In the Web Console, you can change the [log server](#) address to which the Kaspersky Thin Client [event and audit logs](#) are forwarded.

To configure forwarding of Kaspersky Thin Client logs to the log server via the Web Console:

1. In the main window of the Web Console, select **Assets (Devices) → Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with information about Kaspersky Thin Client.

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

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

The screenshot shows the Kaspersky Security Management Suite web console. The top navigation bar includes 'General', 'Events', 'Event configuration', and 'Application settings'. The left sidebar lists 'General', 'System', 'App management', 'Personalization', 'Data exchange' (highlighted), and 'Connections'. The main content area is titled 'Data exchange' and contains three sections: 'Logging' with a 'Log forwarding address' field (placeholder: 'https://example.com or example.com'), 'Confirm user actions' with a text description and a 'Generate confirmation code' button, and 'Remote management' with radio button options for 'Remote connection' and 'Access to remote session'.

Window for configuring forwarding of Kaspersky Thin Client logs via the Web Console

7. In the **Log forwarding address** field, enter the address of the destination log server in the format `https://<server address>`.

To receive event and audit logs from Kaspersky Thin Client, your organization must have a deployed log server that meets the [hardware and software requirements](#).

8. Click **Save** in the lower part of the window.

The changes are saved and applied to Kaspersky Thin Client installed on a thin client after synchronizing Kaspersky Thin Client and Kaspersky Security Center.

Kaspersky Thin Client personalization: one device

In the Web Console, you can upload your images and set them as desktop background or lock screen of Kaspersky Thin Client. The following file formats are supported: JPEG, PNG, JPG. The maximum file size is 15 MB. You can also delete uploaded images from the Web Console.

By default, a standard background is set on the desktop and the lock screen of Kaspersky Thin Client. If you've set a background, you can reset your personalization settings to revert to the default background.

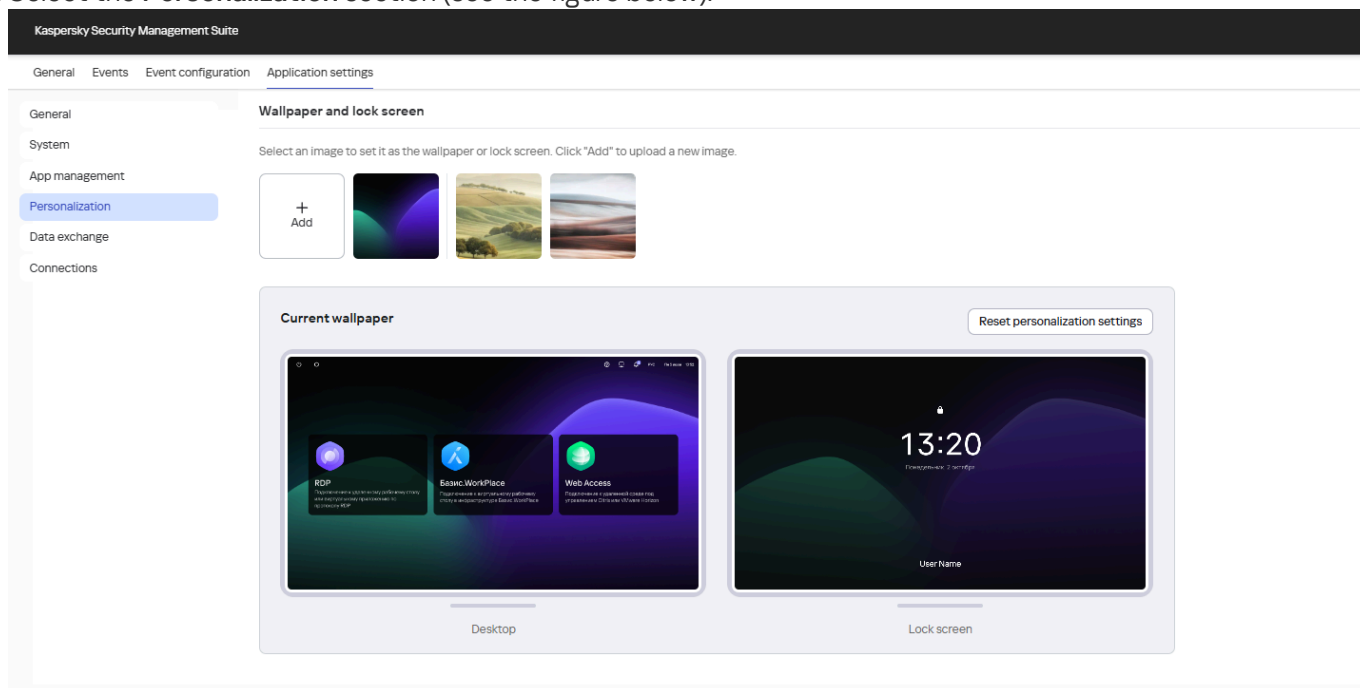
You cannot change the background in the Kaspersky Thin Client interface. Instead, you can change the background of screens only via the Web Console. The image set via the Web Console also changes to the standard background [if the factory reset is made](#).

To change the lock screen or desktop background of Kaspersky Thin Client:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with information about Kaspersky Thin Client.
5. Select the **Application settings** tab.
6. Select the **Personalization** section (see the figure below).



Window for configuring personalization settings of Kaspersky Thin Client via the Web Console

7. To change your desktop or lock screen background, follow these steps:

a. Select the image you want to set as a background.

- If you want to upload a new image to the Web Console, click the **Add** button.
In the window that opens, drag the desired image to the upload area or click **Upload a file or drag and drop it here**, then select the desired image in the window that opens.
- If you want to use an image that has already been uploaded to the Web Console, click the image's thumbnail.

A preview window will appear for the placement of the selected image on the Kaspersky Thin Client screens.

If you want to save the image in the Web Console without setting it as the background, go to step c. of these instructions.

b. Check the boxes next to the screens on which you want to set the image as a background:

- **Desktop:** the image will be set as the [desktop background of Kaspersky Thin Client](#).
- **Lock screen:** the image will be set as the [lock screen background](#).

c. Click **Save** in the preview window.

The main screen of the **Personalization** section will be displayed. The background will be set to screens you selected.

8. To delete an image uploaded to the Web Console, hover over the image's thumbnail and click the  button that appears.

Confirm your actions in the window that appears.

The image will be permanently deleted from the Web Console. If the image was selected as the background on any screen, the standard background will be set in its place.

9. To revert all screens to standard background, click **Reset personalization settings** and confirm your actions in the window that opens.

A standard background will be set on the desktop and the lock screen of Kaspersky Thin Client.

10. Click **Save** in the lower part of the **Personalization** section window.

The changes will be saved and applied to the thin client within an hour after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

Configuring settings for remote connection to a thin client via the Web Console: one device

In the Web Console, you can configure the following settings for remote connection to a thin client:

- Remote management access mode: determines the conditions and procedure for connecting to the thin client.
- The mode of access to the remote session running on the thin client when the connection to it is established (hereinafter also referred to as the "remote environment screen").

It may be necessary to restrict access to the remote environment screen if the thin client user is working with sensitive or confidential data.

To configure settings for remote connection to a thin client:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with information about Kaspersky Thin Client.
5. Select the **Application settings** tab.
6. Select the **Data exchange** section (see the figure below).

Window for configuring the remote thin client management via the Web Console

7. In the **Remote management** section, select the access mode for remote management of the thin client:

- **Allow automatically**

In this mode, the administrator will be able to remotely connect to the thin client after the user [accepts the remote management request in the Kaspersky Thin Client interface](#). If the user rejects the request, the connection is terminated. If there is no response within 30 seconds, the connection is established automatically.

- **Allow by request**

In this mode, the administrator will be able to remotely connect to the thin client only after the user [accepts the remote management request in the Kaspersky Thin Client interface](#). If the user rejects the request, the connection is terminated.

- **Deny**

In this mode, the administrator will not be able to remotely connect to the thin client.

If you set the **Allow automatically** or **Allow by request** mode, the **Access to remote session** settings group will be unlocked.

8. In the **Access to remote session** settings group, select the mode of access to the remote environment screen:

- **Allow automatically**

In this mode, after connecting to the thin client, the administrator will be able to access the remote environment screen without user confirmation.

- **Allow by request**

In this mode, after connecting to the thin client, the administrator will be able to access the remote environment screen only after the user [accepts this access request in the Kaspersky Thin Client interface](#).

- **Deny**

In this mode, the administrator will not be able to remotely manage the thin client until the user manually terminates the remote session.

9. Click **Save** in the lower part of the window.

The changes are saved and applied to Kaspersky Thin Client installed on a thin client after synchronizing Kaspersky Thin Client and Kaspersky Security Center.

Configuring automatic startup and display of applications: one device

In the Web Console, you can select an [application](#) that will be automatically started after turning on the thin client and booting the system, and you can specify which applications will be displayed on the Kaspersky Thin Client desktop.

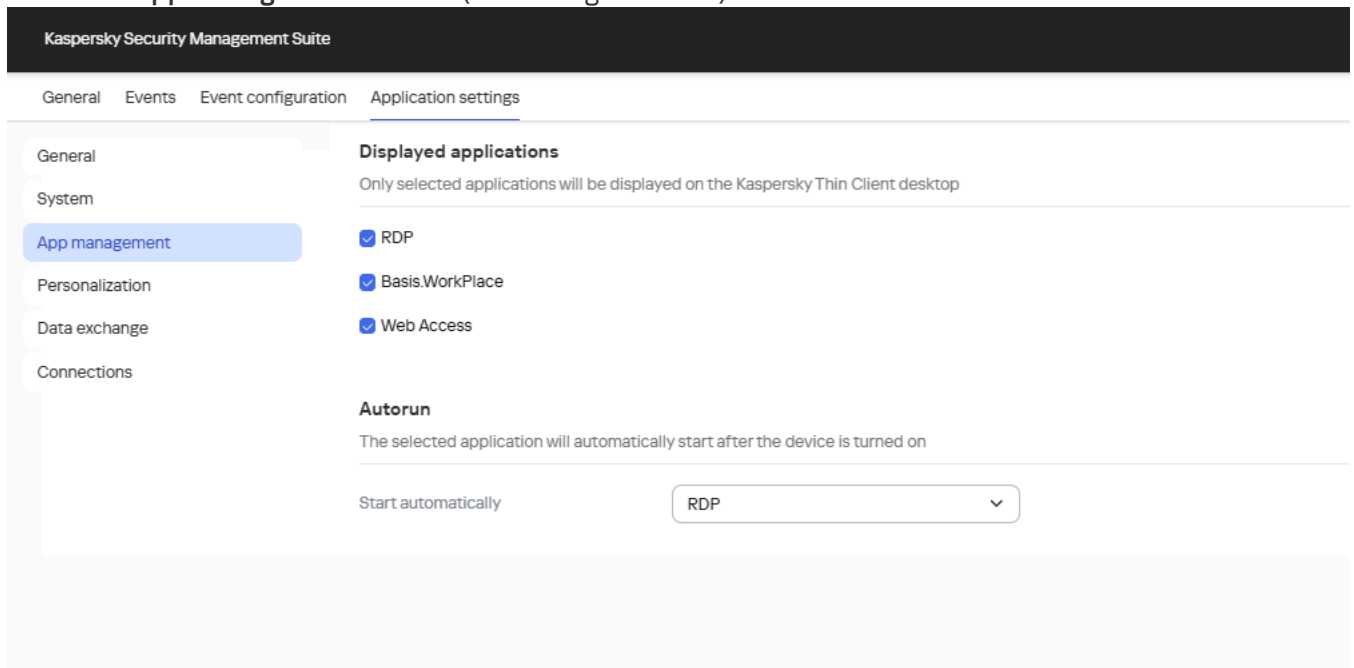
To configure automatic startup and display of applications:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with information about Kaspersky Thin Client.
5. Select the **Application settings** tab.

6. Select the **App management** section (see the figure below).



Configuration window for automatic startup and display of applications via the Web Console

7. In the **Displayed applications** block, select the check boxes next to the applications that will be displayed on the Kaspersky Thin Client desktop.

In the **Start automatically** drop-down list, select the application that will be automatically started after turning on the device and booting the system. If you select **Disabled**, automatic startup will be turned off.

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

The changes are saved and applied to Kaspersky Thin Client installed on a thin client after synchronizing Kaspersky Thin Client and Kaspersky Security Center.

Configuring Kaspersky Thin Client settings for an administration group via the Web Console

In the Web Console, you can use [policies](#) to configure the settings of Kaspersky Thin Client installed on thin clients that are connected to Kaspersky Security Center and have been added to an [administration group](#).

Configuring the main Kaspersky Thin Client settings via the Web Console: administration group

In the Web Console, you can use [policies](#) to assign names to thin clients in an [administration group](#) and specify the administrator's contact details that will be displayed in the interface of Kaspersky Thin Client installed on these devices.

To configure the main settings of Kaspersky Thin Client via the Web Console:

1. In the main window of the Web Console, select **Assets (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).

The screenshot shows the 'Kaspersky Security Management Suite' interface. At the top, there are tabs: 'General', 'Event configuration', 'Application settings', and 'Revision history'. The 'General' tab is selected. On the left, there is a sidebar with a list of settings: 'General', 'System', 'App management', 'Personalization', 'Data exchange', 'Connections', and 'Certificates'. The 'General' section is expanded. The main content area is divided into two sections. The first section is 'Group device naming rule', which states: 'All devices in the group will have a compound name. Example: Accounting-00000001-Voronezh.' Below this, there are two input fields: 'Name' (with a placeholder 'Enter name') and 'Suffix' (with a placeholder 'Enter additional information'). The second section is 'Technical support contacts', which states: 'Users will see these contact details in the Kaspersky Thin Client interface.' Below this, there is a 'Contact details' field with a placeholder: 'Specify the phone number and email address of your company's technical support or system administrator'.

Window for configuring the main settings of Kaspersky Thin Client installed on thin clients in an administration group via the Web Console

5. Configure the required settings:

- In the **Group device naming rule** section, enter the name and additional information in the relevant fields. This data is displayed in the name of each thin client added to the administration group. You can enter uppercase and lowercase letters in Cyrillic or Latin and special characters. Maximum text length in each field: 10 characters.
The names of thin clients also include an identifier (ID). This is a unique set of eight characters that is automatically generated for each device added to the administration group. You can [change the identifier of an individual thin client](#).
- In the **Technical support contacts** section, in the **Contact details** field, enter the phone number and name of the administrator or, for example, the email address of your technical support service. The number of characters in this field must not exceed 80 characters.
The entered information is displayed for thin clients added to an administration group in the Kaspersky Thin Client interface: in the control panel, 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](#).

6. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.
7. Click **Save** in the lower part of the window.

The changes will be saved and applied to Kaspersky Thin Client installed on the thin clients added to the administration group after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

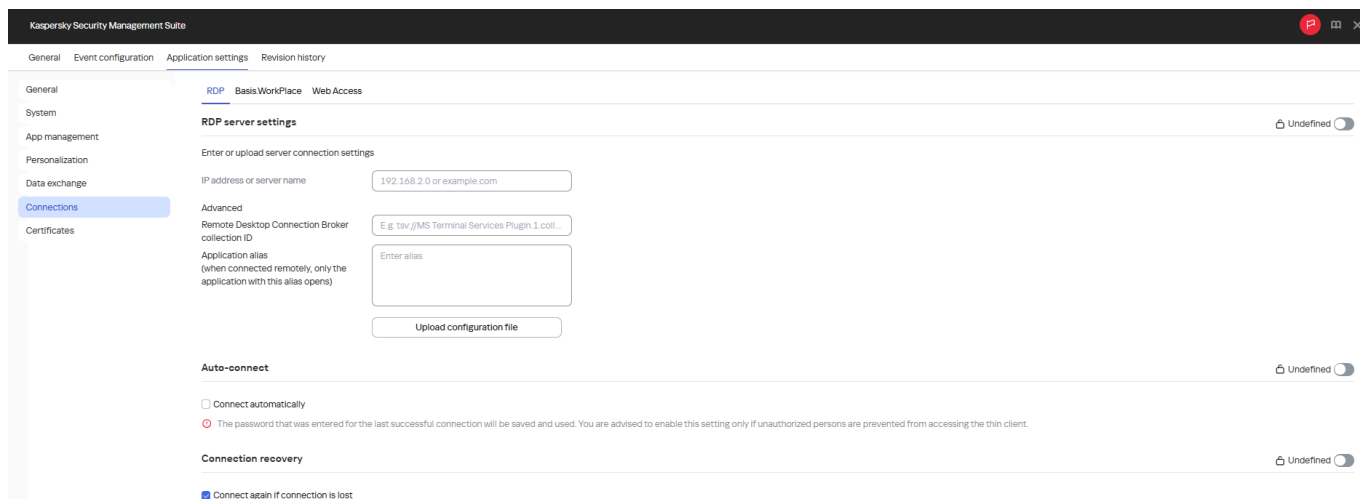
Configuring a connection to a remote environment using the RDP application via the Web Console: administration group

In the Web Console, you can use [policies](#) to configure settings for [connecting to a remote environment using the RDP application](#).

To configure the settings for connecting to a remote environment using the RDP application:

1. In the main window of the Web Console, select **Assets (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 environment (see the figure below).

The screenshot shows the 'Kaspersky Security Management Suite' web console interface. On the left is a sidebar menu with categories like General, System, App management, Personalization, Data exchange, Connections (highlighted), and Certificates. The main area has tabs for 'General', 'Event configuration', 'Application settings' (selected), and 'Revision history'. Under 'Application settings', there are sub-tabs for 'RDP', 'Basis Workplace', and 'Web Access'. The 'RDP' tab is active, displaying 'RDP server settings'. It includes a toggle for 'RDP server settings' (currently 'Undefined'). Below this is a section for 'Enter or upload server connection settings' with a text field for 'IP address or server name' (containing '192.168.2.0 or example.com') and an 'Advanced' section with a 'Remote Desktop Connection Broker collection ID' field (containing 'E.g. tsv://MS Terminal Services Plugin.1.col...') and an 'Application alias' field (with a note: 'when connected remotely, only the application with this alias opens'). There is an 'Upload configuration file' button. Further down is an 'Auto-connect' section with a toggle (currently 'Undefined') and a checkbox for 'Connect automatically' (unchecked). A warning message states: 'The password that was entered for the last successful connection will be saved and used. You are advised to enable this setting only if unauthorized persons are prevented from accessing the thin client.' At the bottom is a 'Connection recovery' section with a toggle (currently 'Undefined') and a checkbox for 'Connect again if connection is lost' (checked).

Window for configuring a connection to a remote environment in the RDP application via the Web Console: administration group

5. In the **IP address or server name** field, enter the IP address or name of the server for connecting to a remote environment via RDP.
6. If you need 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 need to start a virtual application, specify the application alias in the **Application alias** field.

If you have a configuration file containing the settings for connecting to the Microsoft Remote Desktop Connection Broker and, if needed, the name of the application to open, upload the file by clicking **Upload configuration file**. In this case, you do not have to complete the **Remote Desktop Connection Broker collection ID** and **Application alias** fields.

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. In the **Device redirection** settings block, select the devices to be redirected to the remote environment: **Smart cards, USB drives, Printers and other devices, Microphone, Audio playback devices, Web camera (video), Scanner**.

Audio volume and other settings are managed from the remote environment.

To correctly redirect USB devices to a remote desktop in the Windows 10 operating system, you must enable Microsoft Remote Desktop Services and allow redirection of Plug and Play devices in the settings of Remote Desktop Services. For Microsoft Windows Server 2016 and 2019, you must also enable remote connections via Remote Desktop Services and allow setting remote management rules in Remote Desktop Services.

9. In the **Image quality** block, select the check boxes next to the graphic settings of the remote desktop that you want to use: **Smooth fonts, Menu animation, Desktop background, Show window contents while dragging, Enhanced theme**.

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

10. 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.
11. To improve performance when connected to remote desktops or applications, in the **Performance** block, check **Improve graphics performance**.
12. To automatically connect to a remote desktop or virtual application when the RDP application is started, in the **Auto-connect** block, select the **Connect automatically** check box.

To activate the function, the user must manually connect to and disconnect from the remote environment once. When you do so, the following data for connecting to the RDP server is saved in the thin client storage: user name, server address, and password. The next time you start the RDP application, these credentials will be used to automatically initiate a connection to the remote environment. If you disable the auto-connect function, the saved password is deleted from the device storage.

The Web Console does not let you set a password for connecting to a remote environment.

To automatically connect to the remote environment in the RDP application immediately after booting Kaspersky Thin Client, [configure automatic startup of the application](#).

13. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.
14. Click **Save** in the lower part of the window.

The changes will be saved and applied to Kaspersky Thin Client installed on the thin clients added to the administration group after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

Configuring a connection to a remote environment using the Basis.WorkPlace application via the Web Console: administration group

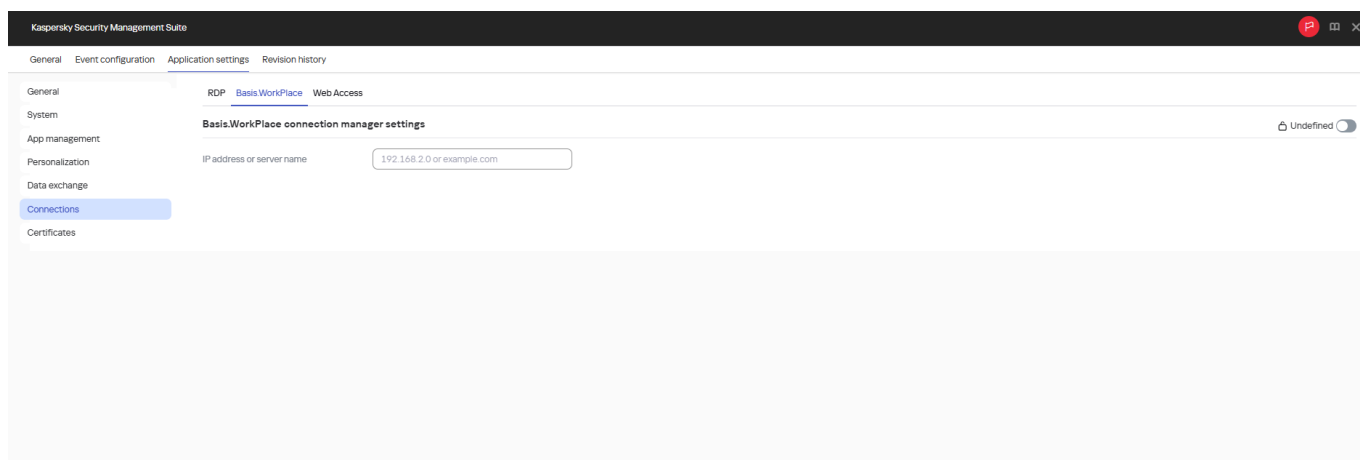
In the Web Console, you can use [policies](#) to configure settings for [connecting to a remote environment deployed in the Basis.WorkPlace infrastructure](#).

Users cannot initiate a password change in Kaspersky Thin Client.

To configure settings for connecting to a remote environment deployed in the Basis.WorkPlace infrastructure:

1. In the main window of the Web Console, select **Assets (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 environment (see the figure below).



Window for configuring a connection to a remote environment deployed in the Basis.WorkPlace infrastructure via the Web Console: administration group

5. In **IP address or server name**, enter the IP address or server name to connect to.
6. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.
7. Click **Save** in the lower part of the window.

The changes will be saved and applied to Kaspersky Thin Client installed on the thin clients added to the administration group after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

Configuring a connection to a remote environment using the Web Access application via the Web Console: administration group

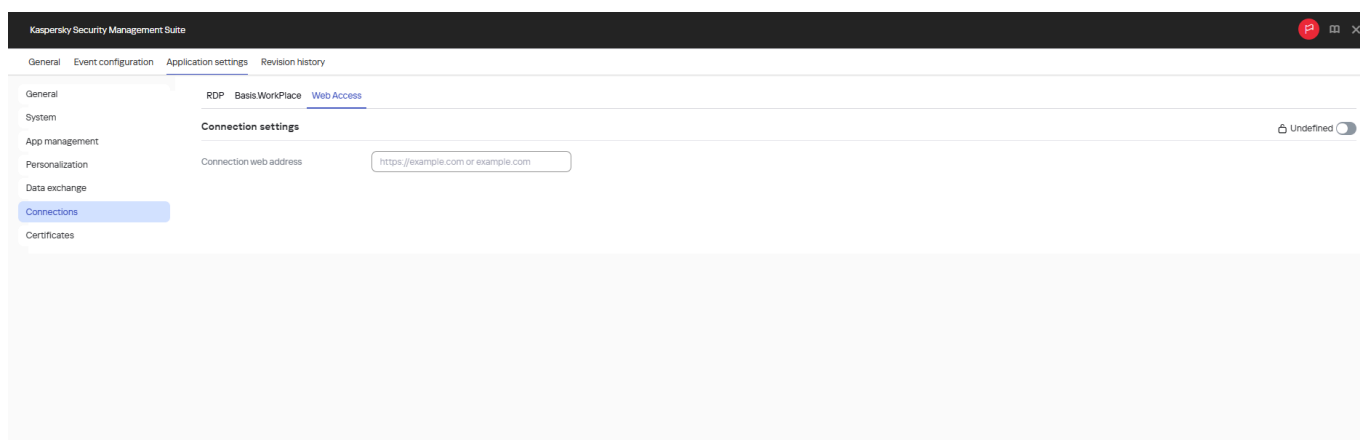
In the Web Console, you can use [policies](#) to configure settings for [connecting to a remote environment using the Web Access application](#).

Using the Web Access application, you can connect to a remote environment deployed in the Citrix Workspace infrastructure. Web Access supports HTML5 and provides a secure HTTPS connection when connecting.

To configure the settings for connecting to a remote environment using the Web Access application:

1. In the main window of the Web Console, select **Assets (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** → **Web Access**.

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



Window for configuring a connection to a remote environment using the Web Access application via the Web Console: administration group

5. In the **Connection web address** field, enter the server web address for connecting to the required remote environment.
6. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.
7. Click **Save** in the lower part of the window.

The changes will be saved and applied to Kaspersky Thin Client installed on the thin clients added to the administration group after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

Configuring monitors and screens via the Web Console: administration group

In the Web Console, you can use [policies](#) to configure monitors connected to thin clients and the settings of Kaspersky Thin Client screens.

Kaspersky Thin Client supports connection of two monitors. The system considers one of the monitors as primary and the other as secondary. During a [remote session](#), the connection panel is displayed on the primary monitor screen. The secondary monitor screen extends or duplicates the image of the primary monitor. In the Web Console, you can select which monitor should be considered the primary monitor (hereinafter also "change the monitor layout").

In the Web Console interface, monitors are numbered. The system determines monitor numbers based on the connection port: monitor 1 is the one nearest to the power source, and monitor 2 is the next one. Refer to the device manufacturer's documentation for the location of the ports on [supported thin client models](#).

The Web Console does not display information about how many monitors are connected to a specific thin client.

If you want the remote session screen to be displayed on both monitors, enable them in the remote environment connection settings in the [RDP](#) or [Basis.WorkPlace](#) applications.

To configure monitors and screens via the Web Console:

1. In the main window of the Web Console, select **Assets (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).

Kaspersky Security Management Suite

General Event configuration Application settings Revision history

General

System

App management

Personalization

Data exchange

Connections

Certificates

System settings of the device Undefined

Interface language English

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

Power-saving settings Undefined

Turn off monitor after 5 minutes

Turn off device after 2 hours

Monitor management Undefined

If the thin client has two monitors connected to it, the system assigns monitor numbers based on the connection port: Monitor 1 is the one nearest to the power source, and Monitor 2 is the next one.

Primary monitor Monitor 1

Display mode Duplicate screen

Monitor 1

Monitor resolution 1024x768

Orientation Landscape

Window for configuring monitors and screens via the Web Console: administration group

5. In the **Monitor management** group, configure the required settings:

- In the **Primary monitor** drop-down list, select which monitor should be considered primary.

If only one monitor is connected to one of the thin clients in the administration group, the settings of the monitor that is set as primary in the Web Console are applied to it.

- In the **Display mode** drop-down list, select the image display option:
 - **Extend screen**—the image spans across two monitors.
 - **Duplicate screen**—the image of the primary monitor's screen is duplicated on the secondary one.

- In the **Monitor resolution** drop-down list, select the desired resolution for the selected screen.

Supported resolutions are listed [in the hardware and software requirements section](#).

If the **Maximum possible** value is selected, the highest value of the parameter supported by the monitor and Kaspersky Thin Client is set.

- In the **Orientation** drop-down list, select the screen position:
 - **Landscape**: the standard screen position.
 - **Landscape flipped**: the screen is rotated 180°.
 - **Portrait**: the screen is rotated 90°.
 - **Portrait flipped**: the screen is rotated 270°.

6. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.

7. Click **Save** in the lower part of the window.

The changes will be saved and applied to Kaspersky Thin Client installed on the thin clients added to the administration group after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

Configuring the Kaspersky Thin Client system settings via the Web Console: administration group

In the Web Console, you can use [policies](#) to configure the interface language and time zone of Kaspersky Thin Client, and to configure the shutdown time for thin clients and monitors connected to them.

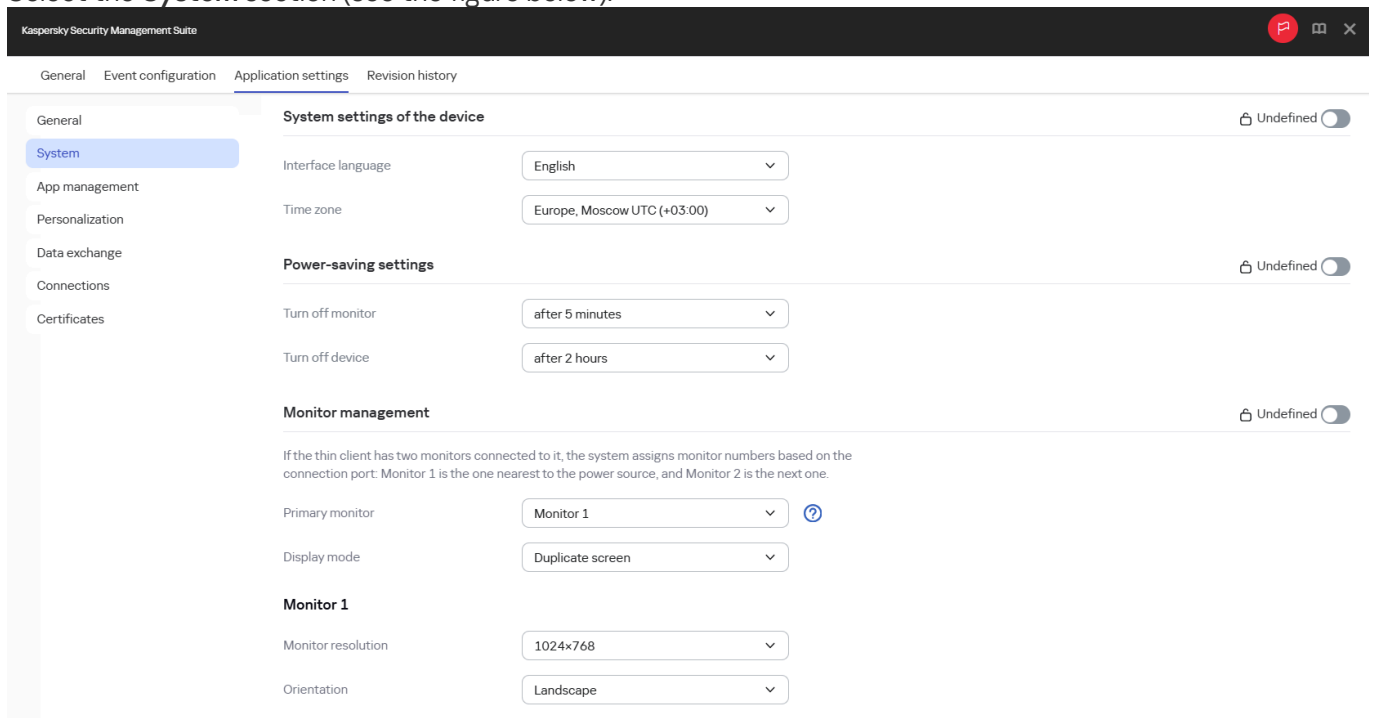
Kaspersky Thin Client 2.3 supports the following interface languages: Russian, English (USA), Spanish (Mexico), and Portuguese (Brazil).

To configure the system settings of Kaspersky Thin Client via the Web Console:

1. In the main window of the Web Console, select **Assets (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).



Window for configuring system settings via the Web Console: administration group

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

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

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

7. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.

8. Click **Save** in the lower part of the window.

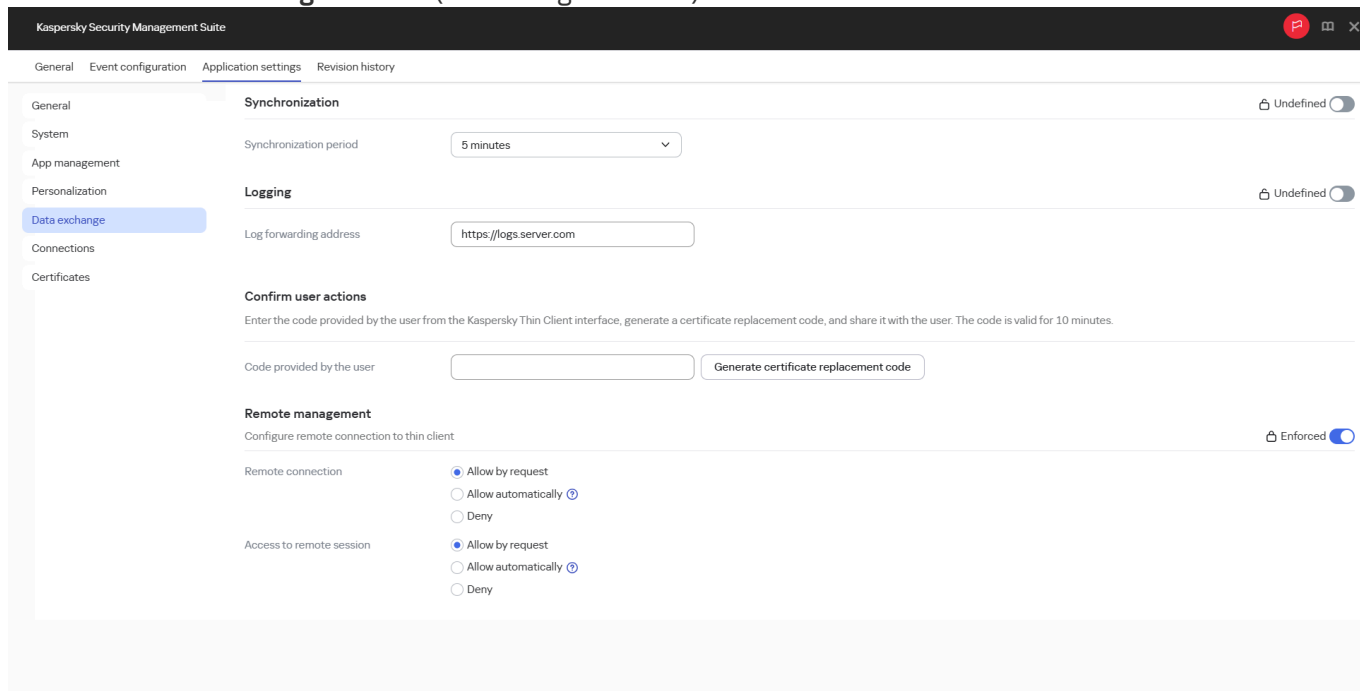
The changes will be saved and applied to Kaspersky Thin Client installed on the thin clients added to the administration group after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

Configuring forwarding of Kaspersky Thin Client logs to a log server: administration group

In the Web Console, you can use [policies](#) to change the [log server](#) address to which the Kaspersky Thin Client [event and audit logs](#) are forwarded.

To configure forwarding of event and audit logs to a log server via the Web Console:

1. In the main window of the Web Console, select **Assets (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).



Window for configuring forwarding of Kaspersky Thin Client logs via the Web Console: administration group

5. In the **Log forwarding address** field, enter the address of the destination log server in the format `https://<server address>`.

To receive event and audit logs from Kaspersky Thin Client, your organization must have a deployed log server that meets the [hardware and software requirements](#).

6. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.
7. Click **Save** in the lower part of the window.

The changes will be saved and applied to Kaspersky Thin Client installed on the thin clients added to the administration group after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

Kaspersky Thin Client personalization: administration group

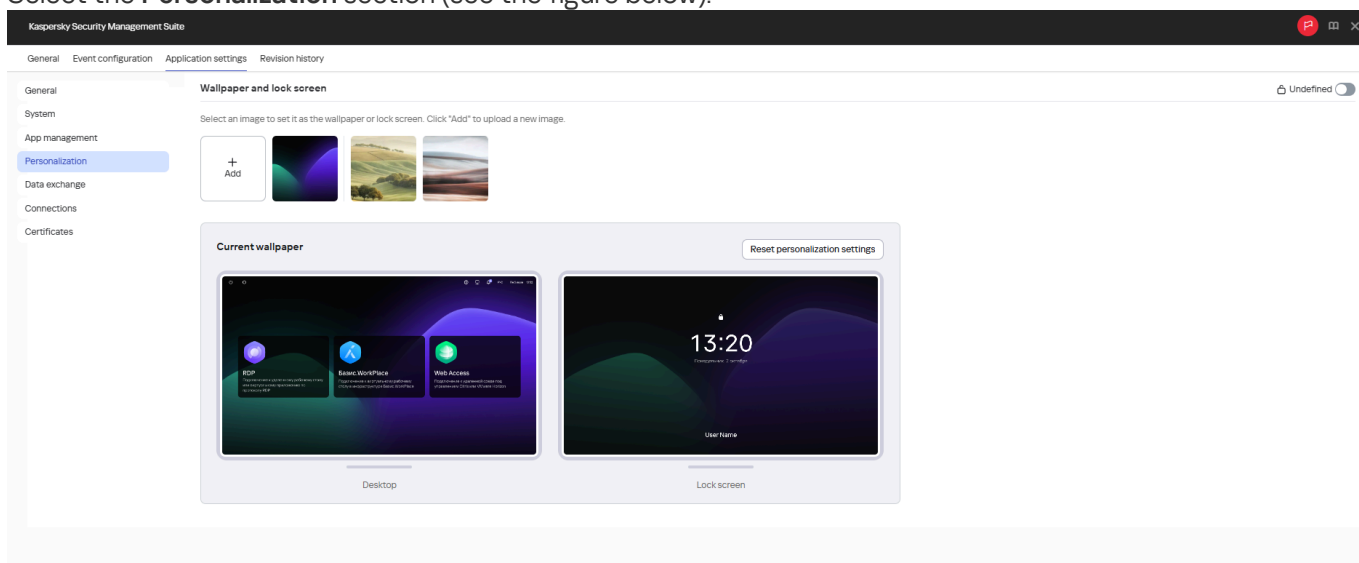
In the Web Console, you can use [policies](#) to upload your images and set them as desktop background or lock screen of Kaspersky Thin Client. The following file formats are supported: JPEG, PNG, JPG. The maximum file size is 15 MB. You can also delete uploaded images from the Web Console.

By default, a standard background is set on the desktop and the lock screen of Kaspersky Thin Client. If you've set a background, you can reset your personalization settings to revert to the default background.

You cannot change the background in the Kaspersky Thin Client interface. Instead, you can change the background of screens only via the Web Console. The image set via the Web Console also changes to the standard background [if the factory reset is made](#).

To change the lock screen or desktop background of Kaspersky Thin Client via the Web Console:

1. In the main window of the Web Console, select **Assets (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 **Personalization** section (see the figure below).



Window for configuring personalization settings of Kaspersky Thin Client via the Web Console: administration group

5. To change your desktop or lock screen background, follow these steps:

- a. Select the image you want to set as a background.
 - If you want to upload a new image to the Web Console, click the **Add** button.
In the window that opens, drag the desired image to the upload area or click **Upload a file or drag and drop it here**, then select the desired image in the window that opens.
 - If you want to use an image that has already been uploaded to the Web Console, click the image's thumbnail.

A preview window will appear for the placement of the selected image on the Kaspersky Thin Client screens. If you want to save the image in the Web Console without setting it as the background, go to step c. of these instructions.

b. Check the boxes next to the screens on which you want to set the image as a background:

- **Desktop:** the image will be set as the [desktop background of Kaspersky Thin Client](#).
- **Lock screen:** the image will be set as the [lock screen background](#).

c. Click **Save** in the preview window.

The main screen of the **Personalization** section will be displayed. The background will be set to screens you selected.

6. To delete an image uploaded to the Web Console, hover over the image's thumbnail and click the  button that appears.

Confirm your actions in the window that appears.

The image will be permanently deleted from the Web Console. If the image was selected as the background on any screen, the standard background will be set in its place.

7. To revert all screens to standard background, click **Reset personalization settings** and confirm your actions in the window that opens.

8. A standard background will be set on the desktop and the lock screen of Kaspersky Thin Client.

9. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.

10. Click **Save** in the lower part of the **Personalization** section window.

The changes will be saved and applied to thin clients added to the administration group within an hour after synchronization of Kaspersky Security Center with Kaspersky Thin Client.

Configuring settings for remote connection to a thin client via the Web Console: administration group

In the Web Console, you can use [policies](#) to configure the following remote connection settings:

- Remote management access mode: determines the conditions and procedure for connecting to the thin client.
- The mode of access to the remote session running on the thin client when the connection to it is established (hereinafter also referred to as the "remote environment screen").

It may be necessary to restrict access to the remote environment screen if the thin client user is working with sensitive or confidential data.

To configure settings for remote connection to a thin client:

1. In the main window of the Web Console, select **Assets (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

App management

Personalization

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 provided by the user from the Kaspersky Thin Client interface, generate a certificate replacement code, and share it with the user. The code is valid for 10 minutes.

Code provided by the user [input] Generate certificate replacement code

Remote management Enforced

Configure remote connection to thin client

Remote connection

☒ Allow by request

☐ Allow automatically ⓘ

☐ Deny

Access to remote session

☒ Allow by request

☐ Allow automatically ⓘ

☐ Deny

Window for configuring a remote connection to a thin client via the Web Console: administration group

5. In the **Remote management** section, select the access mode for remote management of the thin client:

- **Allow automatically**

In this mode, the administrator will be able to remotely connect to the thin client after the user [accepts the remote management request in the Kaspersky Thin Client interface](#). If the user rejects the request, the connection is terminated. If there is no response within 30 seconds, the connection is established automatically.

- **Allow by request**

In this mode, the administrator will be able to remotely connect to the thin client only after the user [accepts the remote management request in the Kaspersky Thin Client interface](#). If the user rejects the request, the connection is terminated.

- **Deny**

In this mode, the administrator will not be able to remotely connect to the thin client.

If you set the **Allow automatically** or **Allow by request** mode, the **Access to remote session** settings group will be unlocked.

6. In the **Access to remote session** settings group, select the mode of access to the remote environment screen:

- **Allow automatically**

In this mode, after connecting to the thin client, the administrator will be able to access the remote environment screen without user confirmation.

- **Allow by request**

In this mode, after connecting to the thin client, the administrator will be able to access the remote environment screen only after the user [accepts this access request in the Kaspersky Thin Client interface](#).

- **Deny**

In this mode, the administrator will not be able to remotely manage the thin client until the user manually terminates the remote session.

7. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.
8. Click **Save** in the lower part of the window.

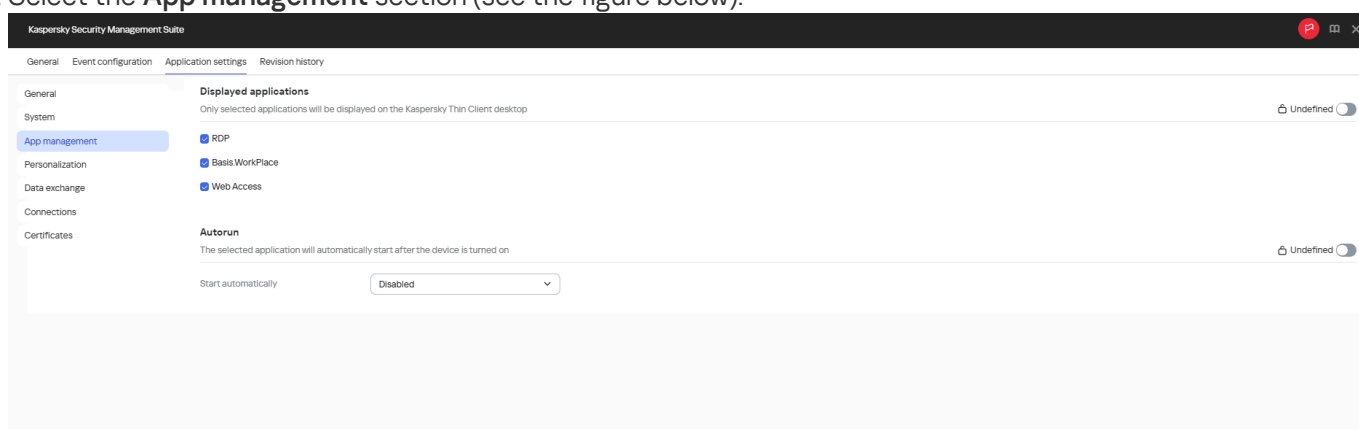
The changes will be saved and applied to Kaspersky Thin Client installed on the thin clients added to the administration group after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

Configuring automatic startup and display of applications: administration group

In the Web Console, you can use [policies](#) to select an [application](#) that will be automatically started after starting the device and booting the system, and you can specify which applications will be displayed on the Kaspersky Thin Client desktop.

To configure automatic startup and display of applications:

1. In the main window of the Web Console, select **Assets (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 **App management** section (see the figure below).



Configuration window for automatic startup and display of applications via the Web Console: administration group

5. In the **Displayed applications** block, select the check boxes next to the applications that will be displayed on the Kaspersky Thin Client desktop.
In the **Start automatically** drop-down list, select the application that will be automatically started after turning on the device and booting the system. If you select **Disabled**, automatic startup will be turned off.
6. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.
7. Click **Save** in the lower part of the window.

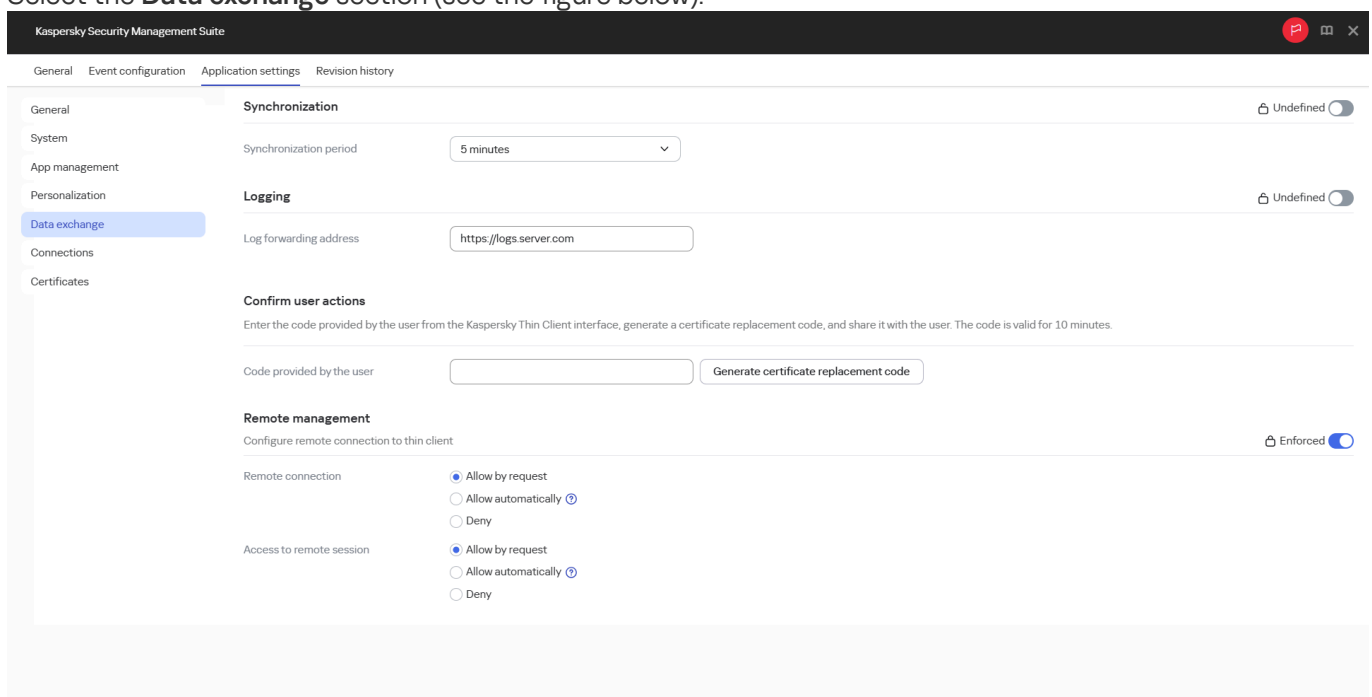
The changes will be saved and applied to Kaspersky Thin Client installed on the thin clients added to the administration group after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

Configuring synchronization between Kaspersky Thin Client and Kaspersky Security Center

In the Web Console, you can configure the synchronization period between Kaspersky Thin Client and Kaspersky Security Center only using [policies](#).

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

1. In the main window of the Web Console, select **Assets (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).



The screenshot shows the 'Kaspersky Security Management Suite' web console interface. The 'Application settings' tab is active, and the 'Data exchange' section is selected in the left sidebar. The main content area displays the following settings:

- Synchronization**: Set to '5 minutes'. A toggle switch on the right is set to 'Undefined'.
- Logging**: 'Log forwarding address' is set to 'https://logs.server.com'. A toggle switch on the right is set to 'Undefined'.
- Confirm user actions**: A section for generating a certificate replacement code. It includes a text input for 'Code provided by the user' and a 'Generate certificate replacement code' button.
- Remote management**: A section for configuring remote connection to thin client. It includes a toggle switch on the right set to 'Enforced'.
- Remote connection**: Radio buttons for 'Allow by request' (selected), 'Allow automatically', and 'Deny'.
- Access to remote session**: Radio buttons for 'Allow by request' (selected), 'Allow automatically', and 'Deny'.

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

5. In the **Synchronization period** drop-down list, select the interval for synchronizing Kaspersky Thin Client with Kaspersky Security Center.
6. If you want the configured settings to be applied to Kaspersky Thin Client installed in child administration groups and do not want them to be available for editing in Kaspersky Thin Client in the current administration group, move the [toggles next to the relevant blocks of settings](#) to the **Enforced** position.
7. Click **Save** in the lower part of the window.

The changes will be saved and applied to Kaspersky Thin Client installed on the thin clients added to the administration group after synchronization of Kaspersky Thin Client with Kaspersky Security Center.

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](#)

If a thin client running Kaspersky Thin Client is not connected to Kaspersky Security Center or is connected but is not included in the [administration group](#), this thin client will not send the administrator any requests to confirm the actions listed above. [Add the thin client to the administration group](#) to receive requests to confirm user actions.

To confirm the change of settings for connecting to Kaspersky Security Center or reset of Kaspersky Thin Client settings:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.
2. In the displayed list, click the name of the relevant thin client. You can view the device name in the [Kaspersky Thin Client interface](#). If the thin client name is not on the list, [add it to an administration group](#).

If a setting you are configuring is locked [in a policy that was created for an administration group](#), you cannot change this setting when configuring the individual device. [Change](#) or [unlock](#) this setting in the policy.

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 with information about Kaspersky Thin Client.
5. Select the **Application settings** tab.
6. Select the **Data exchange** section.
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 **Assets (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.

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 certificates via the Web Console

In Kaspersky Security Center, you can access [certificate](#) management functions to connect thin clients to a log server and to a remote environment. In the Kaspersky Security Center Web Console interface you can view, [add](#), and [delete](#) such certificates.

We recommend configuring the [connection of thin clients in the administration group](#) to a log server and to a remote environment only using certificates that were assigned by the administrator in the Web Console. This will help prevent Kaspersky Thin Client from connecting to untrusted nodes.

This section also provides [instructions on how to manage certificates for connecting Kaspersky Thin Client to Kaspersky Security Center](#).

About a certificate for connecting Kaspersky Thin Client to Kaspersky Security Center

Kaspersky Thin Client uses a *user mobile certificate* (hereinafter also referred to as "certificate") to connect to Kaspersky Security Center. For detailed information about this and other types of certificates used by Kaspersky Security Center, see the [Kaspersky Security Center Online Help](#).

The certificate is created using the *Administration Server quick start wizard* after installing Kaspersky Security Center. The default validity period of an issued certificate is one year.

User mobile certificates are not reissued automatically.

You can [reissue the certificate in the Web Console](#) or [create a new certificate](#) manually and [upload it to the Web Console](#).

When [migrating to a new Kaspersky Security Center Administration Server](#), [create a new certificate manually](#) in order to upload it to the current Server as a reserve certificate and then to the new Server as the primary certificate.

Reissuing a certificate for connecting Kaspersky Thin Client to Kaspersky Security Center using the Web Console

Kaspersky Thin Client uses a user mobile certificate to connect to Kaspersky Security Center. Certificates of this type are not automatically reissued.

To reissue a certificate for connecting Kaspersky Thin Client to Kaspersky Security Center in the Web Console interface:

1. In the menu of the Kaspersky Security Center Web Console, click the  button next to the name of the Kaspersky Security Center Administration Server.
The **Administration Server properties** window opens.
2. Select the **Certificates** subsection.
3. In the window that opens, in the **Administration Server authentication by mobile devices** section, select the required certificate and click **Reissue**.
4. In the window that opens, specify the Server address and indicate when to activate the certificate. Confirm your choice.
5. Click **Save** in the window that opens.

The certificate for connecting Kaspersky Thin Client to Kaspersky Security Center is reissued.

Devices included in the [administration group](#) receive the reissued certificate for connecting to Kaspersky Security Center after Kaspersky Thin Client is synchronized with Kaspersky Security Center. The reissued certificate is saved to the Kaspersky Thin Client certificate storage and can be used as a reserve one to connect thin clients to Kaspersky Security Center when the current certificate expires.

You can also [manually issue a new certificate](#) to connect Kaspersky Thin Client to Kaspersky Security Center.

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

You can manually create a [certificate](#) for connecting Kaspersky Thin Client to Kaspersky Security Center. The created certificate can be used as a primary or a reserve one, for example, when [migrating to a new Kaspersky Security Center Administration Server](#).

We recommend that you familiarize yourself with the Kaspersky Security Center certificate requirements [in the Kaspersky Security Center Online Help](#).

The created certificate must be [uploaded to the Web Console](#).

To create a 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 397 -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 397 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. Minimum password length: 8 characters.

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.

Uploading a certificate for connecting Kaspersky Thin Client to Kaspersky Security Center using the Web Console

After you [create a certificate](#) to connect Kaspersky Thin Client to Kaspersky Security Center, upload this certificate to the Web Console for transfer to the thin clients added to the [administration group](#).

We recommend that you familiarize yourself with the Kaspersky Security Center certificate requirements [in the Kaspersky Security Center Online Help](#).

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  button next to the name of the Kaspersky Security Center Administration Server.
The **Administration Server properties** window opens.
2. Select the **Certificates** subsection.
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:

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

- a. If the user certificate is protected with a password, enter the password.
- b. Select the user certificate file by clicking the **Browse** button in the **Certificate** block.
- c. Select the private key for the user certificate by clicking the **Browse** button in the **Private key** block.

6. Click **Save** to save the certificate being added.

7. 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. Devices included in the administration group receive the new certificate after Kaspersky Thin Client is synchronized with Kaspersky Security Center.

Adding new certificates in the Web Console

In the Web Console, you can add [certificates](#) to connect to a remote environment or to a log server. To do so, the thin client must be [added to an administration group](#).

After adding a certificate for a thin client in the Web Console, all certificates that were previously accepted by a user will be removed from the device certificate store.

To add new certificates via the Web Console:

1. In the main window of the Web Console, select **Assets (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.

If the added certificate is a root certificate, the connection will be established based on the server domain name only.

Removing certificates from the Web Console

In the Web Console, you can remove certificates assigned to thin clients in an [administration group](#).

If you remove all certificates that were [assigned to a group of thin clients](#), the devices from this group will be able to connect to any server, including servers that have not been assigned any certificates.

To remove certificates:

1. In the main window of the Web Console, select **Assets (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.

Updating a certificate when migrating to a new Kaspersky Security Center Server

To [migrate thin clients to a new Kaspersky Security Center Administration Server](#), issue a [certificate](#), save it on the current Kaspersky Security Center Server as a reserve one, and then use it on the new Server as the primary certificate.

To issue and prepare a new certificate:

1. Start the console and go to the folder in which you want to create the certificate.

2. Run the OpenSSL utility and issue the certificate using the following command:

```
openssl req -x509 -sha256 -nodes -days 397 -newkey rsa:2048 -keyout <key file name>.key -out <certificate file name>.crt
```

The generated certificate and key files are saved locally.

3. Package the certificate and the key into a container using the following command:

```
openssl pkcs12 -export -out <container name>.pfx -inkey <key file name>.key -in <certificate file name>.crt
```

4. Enter and repeat the password for the container. This password is required when uploading the certificate to the servers.

As a result, the container file in PFX format is saved locally.

To upload a certificate to the current Kaspersky Security Center Server as a reserve one:

1. Go to the directory where Kaspersky Security Center is installed and launch the console.

2. Run the klsetsrvcert utility and enter the following command:

```
klsetsrvcert -t MR -i <path to the container> -p <container password> -o NoCA
```

You do not need to download the klsetsrvcert utility. The utility is included in the Kaspersky Security Center distribution kit.

After the command execution, Kaspersky Security Center restarts.

The [reserve certificate](#) is uploaded to the Web Console.

To upload the certificate to a new Kaspersky Security Center Server as the main one:

In the console, start the klsetsrvcert utility and run the following command:

```
klsetsrvcert -t M -i <path to the container> -p <container password> -o NoCA
```

After execution of the instructions above, the certificate for connecting to the new Kaspersky Security Center Administration Server is updated.

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

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

Configuring registration of Kaspersky Thin Client event notifications via 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 importance level. Depending on the conditions of its occurrence, an event can be assigned one of the following importance 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. In the main window of the Kaspersky Security Center Web Console, do one of the following:
 - If the thin client is included in an administration group, select **Assets (Devices)** → **Managed devices**.
 - If the thin client has not been added to an administration group, select **Discovery & deployment** → **Unassigned devices**.
2. Click the name of the device where Kaspersky Thin Client is running. You can view the device name in the [Kaspersky Thin Client interface](#).
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 importance of events whose information you want to receive:

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

A table of events for the selected importance 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 importance to the Kaspersky Security Center Administration Server. The default storage time for events is 30 days.

How to configure event notifications for devices in an administration group

1. In the main window of the Web Console, select **Assets (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 importance of events whose information you want to receive:

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

A table of events for the selected importance 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 included 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 importance 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 [Kaspersky Security Center Online Help](#).

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 Kaspersky Security Center Web Console, do one of the following:
 - If the thin client is included in an administration group, select **Assets (Devices)** → **Managed devices**.
 - If the thin client has not been added to an administration group, select **Discovery & deployment** → **Unassigned devices**.
2. Click the name of the relevant device. The device name is indicated in the [Kaspersky Thin Client interface](#).
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 by Kaspersky Thin Client.
- **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.
- **Importance level** shows severity of the event.
- **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 by Kaspersky Thin Client.

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 environment.](#)

If you are unable to resolve the error, please contact [Technical Support](#). If necessary, Technical Support experts may ask you to provide system information or [event and audit logs](#).

Reconnecting after a remote connection failure

In the event of a connection failure between Kaspersky Thin Client and the remote environment, an automatic reconnect will be initiated provided that this feature is activated in the remote connection configuration.

If the connection is not restored during the re-connection attempt or if automatic connection is declined, the remote session screen closes and a message indicating the cause of the malfunction is displayed.

To resume the remote session:

1. Close the error message.
2. Try connecting to the remote environment.
3. If you are unable to connect, reach out to your administrator for help troubleshooting any physical network issues that might be preventing Kaspersky Thin Client from connecting to the remote desktop.
4. If the direct connection is established but you still cannot connect to the remote desktop, please contact [Technical Support](#).

Problems restricting access to the Kaspersky Security Management Suite web plug-in functions

After [installing](#) or [updating](#) the Kaspersky Security Management Suite web plug-in, [users with full set of rights](#) might not have access to some application functions.

To fix problems with shared access to web plug-in functions:

1. Place the RBAC file from the [web plug-in distribution kit](#) into the following directories on the [Administration Server](#):

a. <Kaspersky Security Center installation directory>/rbac

b. /var/opt/kaspersky/klnagent_srv/1093/dat/rbac

2. Restart the Administration Server.

Users must be granted the rights to access the web plug-in functions according to their roles.

If you are unable to fix the problem, please contact [Technical Support](#).

Contacting Technical Support

If you experience problems that [you cannot resolve on your own](#) when working with Kaspersky Thin Client, please contact [Kaspersky Technical Support](#) [↗].

Before contacting Technical Support, please make sure to read the [Technical Support rules](#) [↗].

When you contact Technical Support, experts may ask you to provide [audit and event logs](#). In the Kaspersky Thin Client interface, you can [forward logs to a log server](#) deployed in your organization's infrastructure, from where Kaspersky experts can download them.

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 important events in thin client operation, such as interaction with certificates to connect to Kaspersky Security Center, information about the Administration Server and connections or disconnections from it, and factory resets of the device. The audit log cannot be viewed in the Kaspersky Thin Client interface. You can [forward the audit log file to a log server](#).

Event log

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* is a file name.
 - *Line Number* is a number of the line in the file.
 - *Function* is debug information.
- Process ID and thread ID.
- Product version ID.

Audit log

The Kaspersky Thin Client audit log contains the following events and event details:

- Adding, replacing, and switching certificates for connecting to Kaspersky Security Center in the Kaspersky Thin Client interface:
 - date and time of the event;
 - IP address and/or domain name of the Kaspersky Security Center Administration Server;
 - Kaspersky Security Center Administration Server port number;
 - thin client ID;
 - list of certificate attributes: issuer name, subject name, certificate fingerprint, validity start date and time, validity end date and time.
- Enabling (manually and automatically) and disabling management of Kaspersky Thin Client via Kaspersky Security Center:
 - date and time of the event;
 - IP address and/or domain name of the Kaspersky Security Center Administration Server;
 - Kaspersky Security Center Administration Server port number;
 - thin client ID.
- Factory reset of Kaspersky Thin Client:
 - date and time of the event;
 - thin client ID.
- Accepting a remote connection to the thin client:
 - date and time of the event;
 - IP address and/or domain name of the user who connected to the thin client;
 - name of the user who connected to the thin client.

- Creating a new audit log file in case of log rotation:
 - date and time of the event;
 - thin client ID;
 - Kaspersky Thin Client version.
- Saving and deleting the user password for auto-connection to a remote environment:
 - date and time of the event;
 - user name for connecting to the remote environment.

Log forwarding

When you [contact Technical Support](#), Kaspersky experts may ask you to provide [event and audit logs](#). In the Kaspersky Thin Client interface, you can forward logs to a log server, from where the experts can download them.

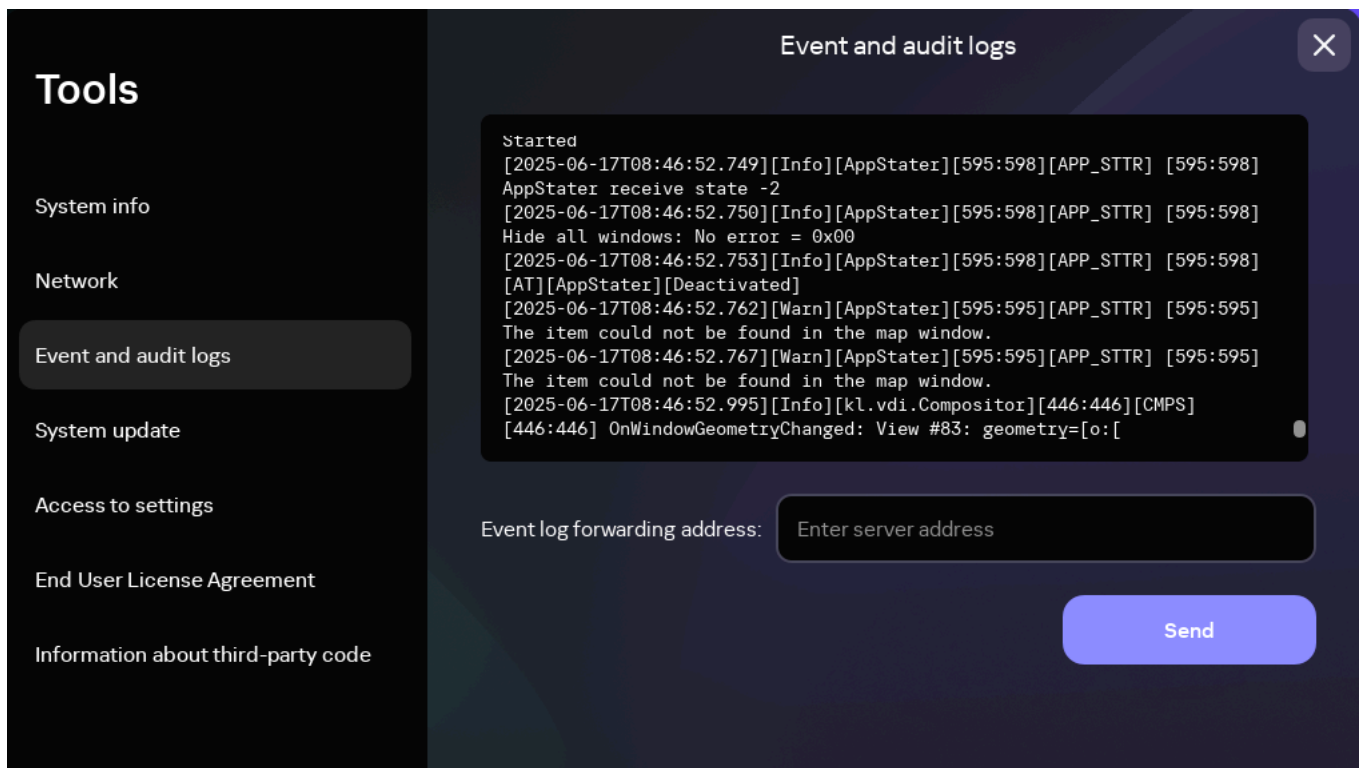
The [log server](#) must first be deployed in your organization's infrastructure. For detailed information on server deployment, please refer to the Administrator's Guide for this server.

The maximum file sizes for the event log and audit log are 150 MB and 512 MB, respectively. When the file size of the event or audit log 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 and audit logs** section (see the figure below).

This section displays the event log entries. Audit log entries are not displayed in the Kaspersky Thin Client interface.



Tools. Event and audit logs 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 the thin client belongs to an [administration group](#), the log server address can be [enforced via the Web Console](#). If this is the case, you will not be able to change it in the Kaspersky Thin Client interface.

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 exposed to third parties.

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

If the device is not a member of an [administration group](#) and this is the first time you are sending event and audit logs to the log server, you will see a window prompting you to add a [certificate to connect to the log server](#).

Check the settings of the certificate that you are adding 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.

Glossary

Administration group

A set of devices managed by Kaspersky Security Center and grouped by function. Devices are grouped for easy management as a whole. A group may include other groups. For each device added to the group, you can create group policies and group tasks that will apply to all devices in the 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.

Broker

Service that controls access and connections to remote desktops and applications (for example, Microsoft Remote Desktop Connection Broker).

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.

Log server

The server that will receive Kaspersky Thin Client [event and audit logs](#). This server is deployed within your corporate network.

Policy

A policy determines settings of Kaspersky Thin Client and defines access to configuration of Kaspersky Thin Client system settings on devices within an administration group. You can create an unlimited number of different policies for Kaspersky Thin Client 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.

Remote desktop

An operating system that is either installed on a computer or deployed in a virtual environment. Remote access technologies are used to connect to this type of operating system.

Remote environment

Any supported remote resource, such as a remote desktop or virtual application, that a thin client user can access for work using remote access technology.

Remote session

Work session in the remote environment the user has connected to through the thin client interface.

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. Peripherals, such as a monitor, keyboard, and mouse, are connected to the thin client.

TLS

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

Virtual application

Application that is deployed on a remote server and requires you to use remote access technologies to connect to it.

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.

Ubuntu is a registered trademark of Canonical Ltd.

Citrix, Citrix Workspace are either registered trademarks or trademarks of Cloud Software Group, Inc., and/or its subsidiaries in the United States and/or other countries.

Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries.

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

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

OpenSSL is a trademark owned by the OpenSSL Software Foundation.

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