Kaspersky Thin Client

Kaspersky Thin Client is an architecture-level secure operating system for thin clients based on KasperskyOS. These thin clients are designed to provide users with remote desktop access and serve as a substitute for a local workstation.

Kaspersky Thin Client uses the **Kaspersky Security Center** console for centralized and secure management of thin client infrastructure. The same console is also used to manage other Kaspersky products. The **Kaspersky Security Management Suite** extension module is provided to connect thin clients to the console.

Flexible thin client management

Centralized management system	The Kaspersky Security Center console is used to: • Configure thin clients • Upgrade thin client • Collect system events from thin clients for auditing and troubleshooting.
Automatic configuration	Fast integration of thin clients into the infrastructure through automatic connection and import of settings from Kaspersky Security Center.
Remote access and management	Connection to a thin client via RDP protocol with authorization capability.
Limited access rights to administration settings	Each administrator can only access thin client management settings relevant to their work responsibilities.
Flexible reporting	• Customizable reports with dynamic filtering and sorting by any data field. • Informative dashboard enabling quick retrieval of all necessary information.
Managing thin client settings	• Rollback of thin client settings to factory defaults. • Disabling of user access to thin client settings. • Centralized control of monitor settings, including changing the desktop background and thin client lock screen.
Compatibility with Kaspersky Security Center	Supports Kaspersky Security Center versions: 15.2

Protection of thin clients from cyberattacks

Inherent security (Security by Design)	The secure-by-design principle inherent in Kaspersky Thin Client architecture and the use of Cyber Immune methodology during development eliminates the likelihood of vulnerabilities being exploited – which is common amongst thin clients from other vendors.
Secure data transfer	Ensures the integrity of data transmitted between users, the remote desktop, centralized management server, and remote desktop infrastructure and log servers. No need for additional security measures.
Secure update	• Centralized automatic updates using Kaspersky Security Center. • The administrator can centrally review and accept the EULA for new versions of KTC and manage the delivery of updates to thin clients.
Network connection control	Certificates are used to control: • User connection to remote desktops and brokers • Connection of thin clients to the centralized management system and log server.
Backup certificates for Kaspersky Security Center	The Kaspersky Security Center backup certificate is automatically delivered to the Kaspersky Thin Client system's certificate storage, without requiring administrator action.
Secure migration to a new Kaspersky Security Center server	Secure connection of a thin client to Kaspersky Security Center with a certificate that differs from the current one.

Hardware platform

Centerm F620	Compact, high-performance thin client for organizing remote workspaces. Easy to maintain and can be mounted on a stand or behind a monitor (VESA mount).

kasperskyOS

Connection scenarios

Terminal servers and guest operating systems	RDP connection to guest operating systems: • Microsoft Windows 10/11 • Microsoft Windows Server 2016/2019/2022 • Various Linux distributions
Supported remote desktop infrastructures and connection methods	Microsoft Remote Desktop Services: • Windows Server 2016/2019/2022 Basis.WorkPlace: • Windows 10/11 • Windows Server 2016/2019/2022 • Various Linux distributions Citrix and VMware Horizon (via HTML5): • Windows 10/11 • Windows Server 2016/2019/2022 Terminal connection: • Windows Server 2016/2019/2022 (including MS RDS) • Various Linux distributions Direct connection: • Windows 10/11 • Windows Server 2016/2019/2022 • Various Linux distributions
Virtual applications	Supports connection to individual business applications: • Deployed on Microsoft Remote Desktop Services infrastructure (Windows Server 2016/2019/2022) • Deployed on Windows Server 2016/2019/2022 terminal servers • Running on Windows 10/11

User environment

Monitors	Supports up to two monitors (HDMI + DisplayPort or DisplayPort + DisplayPort). Remote desktop image resolution up to FullHD (1920x1080).
USB devices	Forwarding to a remote environment via RDP and HTML5 protocol of the following devices: • Flash drives (including using Client Drive Mapping) • Webcams • USB headsets • Printers, scanners, barcode scanners • USB storage devices for key information — tokens and smart cards (only via RDP).
Wireless input devices (USB interface)	Connecting devices with data transmission via radio channel: • Keyboards • Mice.

Multimedia capabilities

Audio	Playing and sending audio from devices connected to the thin client to the remote desktop.
Video	Redirecting a video stream from a webcam connected to the thin client to the remote desktop.
Audio conferencing	Audio conferencing is supported in VideoMost, IVA Technologies and SPIRIT DSP solutions.

Additional functions

User interface and capabilities	• Customizable Kaspersky Thin Client control panel that does not overlap with important elements of the remote desktop. • Customization of the interface according to individual preferences. • Initial setup wizard for Kaspersky Thin Client operating system. • Extended notification system. For example, the system asks the user for a convenient reboot time. • Detailed error messages with troubleshooting tips. • Automatic reconnection to the remote desktop in the event of a connection failure.
User interface localization	Input language configuration: select only the keyboard layouts required by the user. The following keyboard layouts are available: • Russian • English • Mexican Spanish • Brazilian Portuguese • Deutsch • Swiss German • Swiss French.
Administrator control	The administrator can flexibly control user settings, for example, prohibit the use of microphone, headphones or a second monitor.
Lock screen	The user can lock the remote session screen and thin client interface.
Featured connections	Ability to display only the applications selected in the settings on the thin client desktop (RDP, Basis.WorkPlace, Web Access).
Autostart applications	Automatic launch one of the applications (RDP, Basis.WorkPlace, Web Access) selected by the user after the thin client starts.
Automatic connection	Automatic connection to the remote desktop after launching the RDP application.
Configuration of power saving parameters	Configuring the monitor and thin client to power off when Kaspersky Thin Client is idle.
Deferred installation of updates	The user can postpone the installation of a Kaspersky Thin Client update for a fixed amount of time.

os.kaspersky.com

kasperskyOS