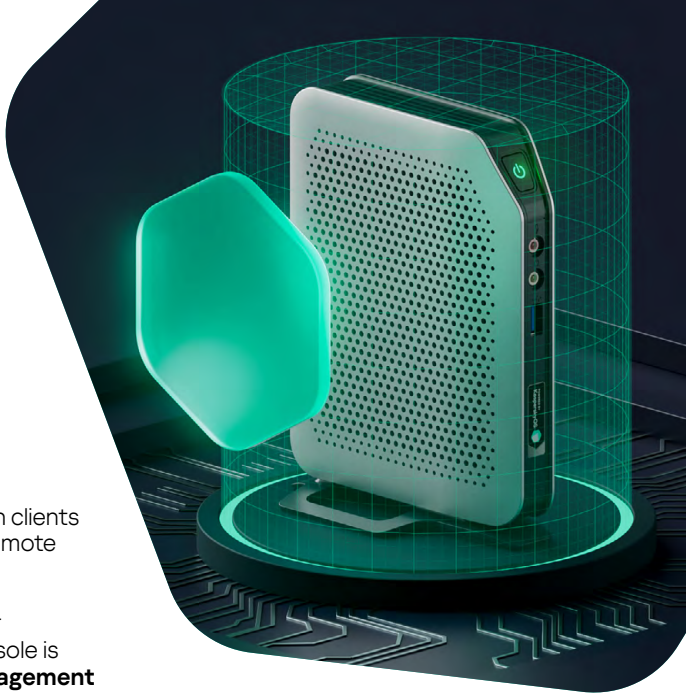
Kaspersky Thin Client



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 unified **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 • check for updates and upgrades of thin clients • 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.
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.
Compatibility with Kaspersky Security Center	Supports Kaspersky Security Center versions: 14.2.
Protection of thin clients from cyberattacks	
Inherent security (Security by Design)	The secure-by-design principles inherent in KasperskyOS architecture and the use of Cyber Immune methodology during development eliminate potential exploitation of a wide range of vulnerabilities typical of 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 from the Kaspersky update server 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	Delivery of the backup certificate to the Kaspersky Thin Client system certificate storage is automatic and transparent for the Kaspersky Security Center administrator.
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.

KasperskyOS

Hardware platform	
Centerm F620	Compact, high-performance thin client for organizing remote workspaces. Features: passive cooling, maintainability, mounted on a stand or behind the monitor (VESA mount).
Connection scenarios	
Terminal servers and guest operating systems	RDP connection to guest operating systems: • Microsoft Windows 7 • Microsoft Windows 10 • Microsoft Windows 11 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 • Microsoft Windows Server 2022 • Astra Linux Common Edition 2.12.43 (Oryol) • Astra Linux Special Edition 1.7 (Smolensk) • Alt Linux 10 • RED OS 7.3
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 • Astra Linux SE 1.7/CE 2.12, ALT Linux 10 and RED OS 7.3 Citrix and VMware Horizon (via HTML5): • Windows 10/11 • Windows Server 2016/2019/2022 Terminal connection: • Windows Server 2016/2019/2022 (including MS RDS) • Astra Linux SE 1.7/CE 2.12, ALT Linux, RED OS 7.3 Direct connection: • Windows 7/10/11 • Windows Server 2016/2019/2022 • Astra Linux SE 1.7/CE 2.12, ALT Linux 10, RED OS 7.3
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
Automatic connection	If the RDP connection is lost, the remote desktop is reconnected automatically.
User environment	
Monitors	Support for up to two monitors via HDMI and DisplayPort. Remote desktop image resolution up to FullHD+ (1920x1200).
USB devices	Forwarding of flash drives, smart cards and tokens connected to the thin client to a virtual Windows desktop.
Audio	Playing and sending audio to the remote desktop operating system.
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 important elements of the remote desktop. • Input language configuration: select only the keyboard layouts required by the user. • Customization of the interface according to individual preferences. • Extended notification system. For example, the system prompts 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.
Administrator control	The administrator can flexibly control user settings, for example, prohibit the use of microphone, headphones or a second monitor.
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
www.kaspersky.com

KasperskyOS