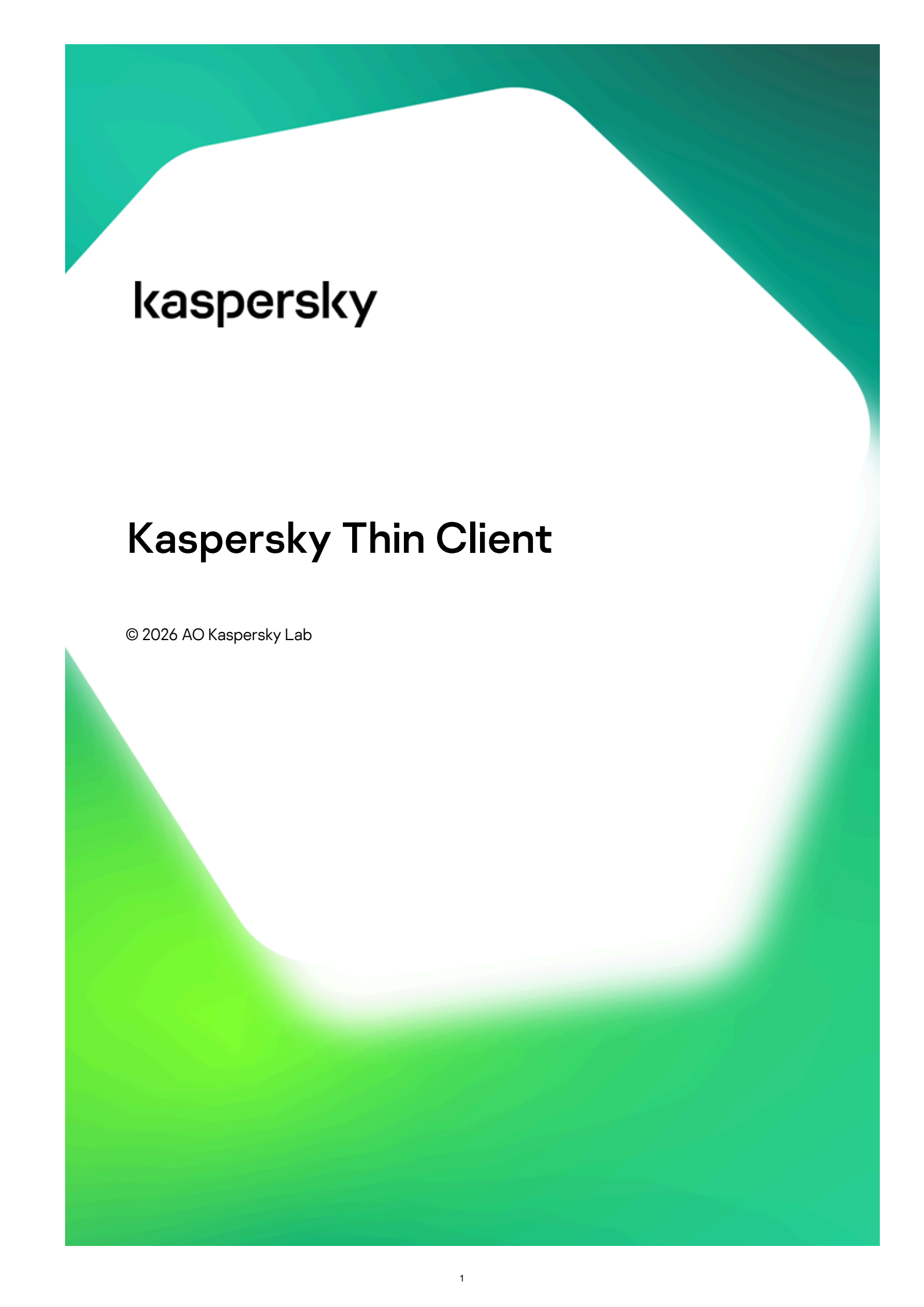


The background of the page is a vibrant green with a white, irregularly shaped cutout in the center. The cutout has rounded corners and a jagged, torn-paper-like edge. The Kaspersky logo and title are positioned within this white area.

kaspersky

Kaspersky Thin Client

© 2026 AO Kaspersky Lab

Contenido

[Ayuda de Kaspersky Thin Client](#)

[Acerca de Kaspersky Thin Client](#)

[Kit de distribución](#)

[Funcionamiento de Kaspersky Thin Client](#)

[Requisitos de hardware y software](#)

[Métodos de conexión remota](#)

[Conexiones mediante la aplicación RDP](#)

[Conexiones mediante la aplicación Basis.WorkPlace](#)

[Conexiones mediante la aplicación Web Access](#)

[Novedades](#)

[Instalar y actualizar Kaspersky Thin Client](#)

[Instalar Kaspersky Thin Client](#)

[Actualizar Kaspersky Thin Client](#)

[Interfaz de Kaspersky Thin Client](#)

[Licencia de Kaspersky Thin Client](#)

[Provisión de datos](#)

[Encender e iniciar Kaspersky Thin Client por primera vez](#)

[Reiniciar y apagar Kaspersky Thin Client](#)

[Uso de certificados en Kaspersky Thin Client](#)

[Configurar Kaspersky Thin Client](#)

[Procedimiento: inicio rápido para administradores](#)

[Procedimiento: asignar certificados a un grupo de clientes ligeros](#)

[Procedimiento: migrar clientes ligeros a un nuevo servidor de Kaspersky Security Center](#)

[Configurar los ajustes generales](#)

[Configurar los ajustes de la red](#)

[Administrar los dispositivos de reproducción y grabación de audio](#)

[Configurar los ajustes para conectar Kaspersky Thin Client a Kaspersky Security Center](#)

[Modificar los ajustes de conexión a Kaspersky Thin Client a Kaspersky Security Center](#)

[Configurar la fecha y la hora](#)

[Configurar el inicio automático y la visualización de aplicaciones](#)

[Configurar los monitores y pantallas](#)

[Configurar los ajustes de ahorro de energía](#)

[Configurar los ajustes para la administración remota de clientes ligeros en la interfaz de Kaspersky Thin Client](#)

[Cambiar el tipo de dispositivos USB no identificados](#)

[Restablecer la configuración de Kaspersky Thin Client](#)

[Configurar los ajustes para conectarse a un entorno remoto usando la aplicación RDP](#)

[Configurar los ajustes para conectarse a un entorno remoto usando la aplicación de Basis.WorkPlace](#)

[Configurar el acceso a los ajustes de Kaspersky Thin Client](#)

Administrar Kaspersky Thin Client en un cliente ligero

Escenario: trabajar en Kaspersky Thin Client en un cliente ligero

Conexión a un entorno remoto

Conectarse a un entorno remoto usando la aplicación RDP

Conectarse a un entorno remoto usando la aplicación Basis.WorkPlace

Conectarse a un entorno remoto usando la aplicación Web Access

Controlar una sesión remota

Utilizar el panel de conexión

Bloquear y desbloquear una sesión remota

Cerrar una sesión remota

Administrar dispositivos de reproducción y grabación de audio en el panel de conexiones

Administrar ventanas de aplicaciones virtuales

Web Access: redirigir dispositivos USB a un entorno remoto

Consultar información sobre Kaspersky Thin Client y un cliente ligero

Ver información sobre el estado de la red

Ver notificaciones de Kaspersky Thin Client

Administrar certificados en la interfaz de Kaspersky Thin Client

Administrar Kaspersky Thin Client mediante combinaciones de teclas

Controlar el acceso a la capacidad de administración remota y a la pantalla del entorno remoto

Conexión remota a un cliente ligero

Administrar Kaspersky Thin Client a través de Kaspersky Security Center Web Console

Acerca del complemento web de Kaspersky Security Management Suite

Instalar el complemento web de Kaspersky Security Management Suite

Actualizar el complemento web Kaspersky Security Management Suite

Eliminar el complemento web Kaspersky Security Management Suite

Restringir el acceso a las funciones del complemento web de Kaspersky Security Management Suite

Iniciar y cerrar sesión en Web Console

Administrar directivas y grupos de administración

Crear un grupo de administración

Agregar clientes ligeros al grupo de administración

Crear una directiva

Modificar una directiva

Bloquear ajustes en una directiva

Configurar los parámetros de Kaspersky Thin Client para un dispositivo a través de Web Console

Cambiar el id. de un cliente ligero a través de Web Console: un dispositivo

Configurar la conexión a un entorno remoto usando la aplicación RDP a través de Web Console: un dispositivo

Configurar la conexión a un entorno remoto usando la aplicación Basis.WorkPlace a través de Web Console: un dispositivo

Configurar una conexión a un entorno remoto en la aplicación Web Access a través de Web Console: un dispositivo

Configuración de monitores y pantallas a través de Web Console: un dispositivo

Configurar los ajustes de sistema de Kaspersky Thin Client a través de Web Console: un dispositivo

Configurar el envío de los registros de Kaspersky Thin Client a un servidor de registros: un dispositivo

Personalizar Kaspersky Thin Client: un dispositivo

Configurar los ajustes para la conexión remota de un cliente ligero a través de Web Console: un dispositivo

Configurar el inicio automático y la visualización de aplicaciones: un dispositivo

Configurar los ajustes de Kaspersky Thin Client para un grupo de administración a través de Web Console

Configurar los ajustes principales de Kaspersky Thin Client a través de Web Console: grupo de administración

Configurar una conexión a un entorno remoto usando la aplicación RDP a través de Web Console: grupo de administración

[Configurar la conexión a un entorno remoto usando la aplicación Basis.WorkPlace a través de Web Console: grupo de administración](#)

[Configurar una conexión a un entorno remoto usando la aplicación Web Access a través de Web Console: grupo de administración](#)

[Configurar los monitores y las pantallas a través de Web Console: grupo de administración](#)

[Configurar los ajustes de sistema de Kaspersky Thin Client a través de Web Console: grupo de administración](#)

[Configurar el envío de los registros de Kaspersky Thin Client a un servidor de registros: grupo de administración](#)

[Personalizar Kaspersky Thin Client: grupo de administración](#)

[Configurar los ajustes para la conexión remota de un cliente ligero mediante Web Console: grupo de administración](#)

[Configurar el inicio automático y la visualización de aplicaciones: grupo de administración](#)

[Configurar la sincronización entre Kaspersky Thin Client y Kaspersky Security Center](#)

[Confirmar las acciones del usuario de Kaspersky Thin Client](#)

[Administrar los certificados de Kaspersky Thin Client a través de Web Console](#)

[Acerca de los certificados para conectar Kaspersky Thin Client a Kaspersky Security Center](#)

[Emitir de nuevo un certificado para conectar Kaspersky Thin Client a Kaspersky Security Center mediante Web Console](#)

[Crear un certificado de usuario para conectar Kaspersky Thin Client a Kaspersky Security Center](#)

[Subir un certificado para conectar Kaspersky Thin Client a Kaspersky Security Center mediante Web Console](#)

[Agregar nuevos certificados en Web Console](#)

[Eliminar certificados de Web Console](#)

[Convertir un certificado del formato PEM al formato DER](#)

[Actualizar un certificado al migrar a un nuevo servidor de Kaspersky Security Center](#)

[Supervisar los eventos de Kaspersky Thin Client a través de Kaspersky Security Center Web Console](#)

[Configurar el registro de notificaciones de eventos de Kaspersky Thin Client a través de Kaspersky Security Center Web Console](#)

[Ver los eventos de Kaspersky Thin Client en Web Console](#)

[Solución de problemas](#)

[Restablecer una conexión remota tras una desconexión](#)

[Problemas al restringir el acceso a las funciones del complemento web de Kaspersky Security Management Suite](#)

[Comunicarse con Soporte técnico](#)

[Acerca de los registros de Kaspersky Thin Client](#)

[Enviar los registros a un servidor](#)

[Glosario](#)

[Administrador de Kaspersky Security Center](#)

[Agente](#)

[Aplicación virtual](#)

[Cliente ligero](#)

[Complemento web Kaspersky Security Management Suite](#)

[Directiva](#)

[Entorno remoto](#)

[Escritorio remoto](#)

[Evento](#)

[Grupo de administración](#)

[Servidor de administración](#)

[Servidor de registros](#)

[Sesión remota](#)

[TLS](#)

[Información sobre código de terceros](#)

[Avisos de marcas comerciales](#)

Ayuda de Kaspersky Thin Client

	Novedades Qué hay de nuevo en esta versión de Kaspersky Thin Client.		Requisitos de hardware y software Entornos remotos y dispositivos periféricos compatibles.
	Instalación y actualización Instalar Kaspersky Thin Client en un cliente ligero. Actualizar la versión de Kaspersky Thin Client.		Primeros pasos Encender el cliente ligero. Realizar la configuración inicial y conectarse a Kaspersky Security Center. Asignar certificados.
	Conexión a un entorno remoto Opciones disponibles para conectarse a un entorno remoto. Conectarse a un entorno remoto. Configurar los ajustes de conexión.		Control centralizado mediante Kaspersky Security Center Web Console Administrar directivas y grupos de administración. Configuración de clientes ligeros con Kaspersky Thin Client.
	Funciones avanzadas Administrar los certificados de Kaspersky Thin Client. Configurar el acceso a los ajustes de Kaspersky Thin Client.		Monitoreo Ver los registros de eventos y de auditoría: enviar estos registros a un servidor de registros. Ver los eventos de Kaspersky Thin Client a través de Kaspersky Security Center Web Console.
	Administración remota Conexión remota a un cliente ligero desde su dispositivo.		Restablecimiento de ajustes y datos Restablecer los ajustes y los datos de Kaspersky Thin Client.

Acerca de Kaspersky Thin Client

Kaspersky Thin Client versión 2.3 (en adelante también denominado "el sistema") es un sistema operativo ciberinmune con micronúcleo. Diseñado para [clientes ligeros](#), el sistema está basado en KasperskyOS. Kaspersky Thin Client está diseñado para conectarse a un entorno remoto y proporcionar un espacio de trabajo en él, y es compatible con dispositivos periféricos conectados al cliente ligero. Kaspersky Thin Client 2.3 puede instalarse en clientes ligeros [Dell™ Wyse 3040](#), [Centerm F620](#) y [TONK TN1200](#).

Este documento no incluye información sobre los componentes de hardware del cliente ligero, como controles y conectores, ya que estos detalles se encuentran en la documentación del vendedor del dispositivo donde está instalado Kaspersky Thin Client.

Principales funciones de Kaspersky Thin Client:

- Conéctese a un entorno remoto:
 - Conéctese a escritorios remotos y virtuales que ejecuten sistemas operativos [Microsoft® Windows®](#) a través del protocolo de escritorio remoto RDP (utilizando, si lo desea, el Agente de conexión a Escritorio remoto de Microsoft).
 - Conéctese a escritorios remotos y virtuales que ejecuten sistemas operativos [Microsoft Windows Server®](#) a través del protocolo de escritorio remoto RDP (utilizando, si lo desea, el Agente de conexión a Escritorio remoto de Microsoft).
 - Conéctese a escritorios remotos y virtuales que ejecuten sistemas operativos [Linux®](#) a través del protocolo de escritorio remoto RDP.
 - Conéctese a aplicaciones virtuales, incluidas aquellas implementadas en la infraestructura de Servicios de Escritorio remoto de Microsoft o que ejecutan sistemas operativos [Microsoft® Windows®](#), a través del Protocolo de Escritorio remoto (RDP).
 - Conéctese a escritorios virtuales desplegados en la infraestructura [Basis.WorkPlace](#).
 - Conéctese a escritorios virtuales desplegados en la infraestructura [Citrix Workspace™](#).
- Transmite imágenes de pantalla del entorno remoto a monitores conectados a un cliente ligero.
- Redirija los siguientes [dispositivos conectados al cliente ligero](#) a un entorno remoto:
 - Teclados y mouses con cable o inalámbricos.
 - Unidades de memoria USB.
 - Dispositivos de reproducción y grabación de audio (auriculares USB).
 - Cámaras web.
 - Tarjetas inteligentes y tokens USB.
 - Dispositivos de impresión y escaneo: impresoras, escáneres (incluidos escáneres de códigos QR y códigos de barras).

- Administre, actualice y supervise de manera centralizada Kaspersky Thin Client a través de [Kaspersky Security Center Web Console](#). El [complemento web de Kaspersky Security Management Suite](#) se utiliza para la comunicación entre Kaspersky Thin Client y Kaspersky Security Center.

Kaspersky Thin Client 2.3 es compatible con Kaspersky Security Center Linux versión 15.3 y Kaspersky Security Center Web Console versión 15.3.

La interfaz de Kaspersky Thin Client 2.3 está disponible en los siguientes idiomas: ruso, inglés (EE. UU.), español (México) y portugués (Brasil).

Kit de distribución

Kaspersky Thin Client 2.3 se entrega en uno de los siguientes formatos:

- Imagen de Kaspersky Thin Client sin una plataforma de hardware (cliente ligero)
- Plataforma de hardware con Kaspersky Thin Client preinstalada entregada por socios

El kit de distribución de Kaspersky Thin Client sin plataforma de hardware incluye los siguientes archivos:

- `Kaspersky_Thin_Client_2.3.0.<versión de compilación técnica>_Wyse3040.tar.gz`: archivo que contiene la imagen de instalación de Kaspersky Thin Client para la plataforma Dell Wyse 3040.
- `Kaspersky_Thin_Client_2.3.0.<versión de compilación técnica>_TN1200.tar.gz`: archivo que contiene la imagen de instalación de Kaspersky Thin Client para las plataformas TONK TN1200 y Centerm F620.
- `hw_install.sh`: script para la instalación en el cliente ligero.
- Scripts para actualizar de las versiones comerciales 2.0 y 2.0.1 a la versión 2.3:
 - `hw_update.sh`
 - `save_files.sh`
 - `restore_files.sh`
- `KTC_LegalNotices_en.txt`: archivo de texto que contiene información sobre código de terceros.
- Archivos de texto que describen las nuevas funciones y las limitaciones conocidas:
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<versión de compilación técnica>_EN.txt`
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<versión de compilación técnica>_ES.txt`
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<versión de compilación técnica>_PT_BR.txt`
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<versión de compilación técnica>_RU.txt`
- Archivos del Contrato de licencia de usuario final de Kaspersky Thin Client:
 - `eula_en_ktc_00008.txt`
 - `eula_es_ktc_00008.txt`

- eula_pt_ktc_00008.txt
- eula_ru_ktc_00008.txt

El kit de distribución de Kaspersky Security Management Suite versión 2.3 se entrega con los componentes enumerados más abajo.

Si descomprime el archivo de almacenamiento utilizando una herramienta de automatización (por ejemplo, un script), deberá leer y aceptar los términos y condiciones del Contrato de licencia de usuario final antes de usar Kaspersky Security Management Suite.

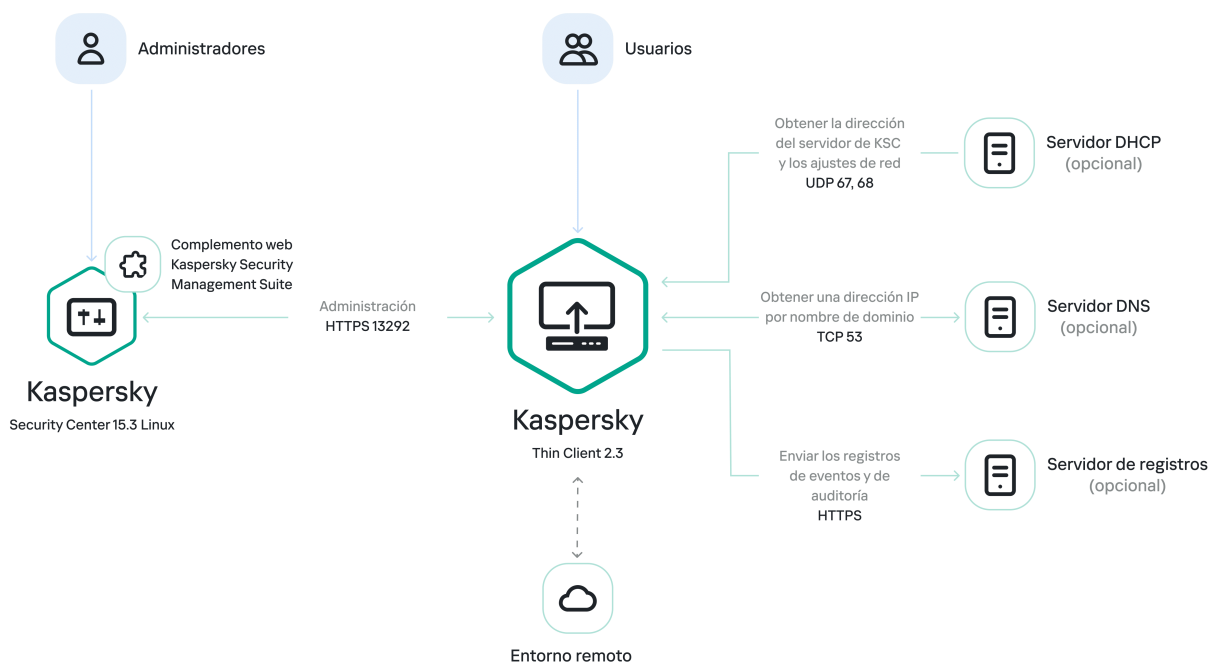
- Archivos para Linux que contienen las imágenes de instalación y los archivos de firma del complemento web para Kaspersky Security Center:
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versión de compilación técnica>_en.sh
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versión de compilación técnica>_es.sh
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versión de compilación técnica>_pt_br.sh
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versión de compilación técnica>_ru.sh
- Archivos para Microsoft Windows que contienen las imágenes de instalación y los archivos de firma del complemento web para Kaspersky Security Center:
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versión de compilación técnica>_ru.exe
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versión de compilación técnica>_en.exe
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versión de compilación técnica>_es.exe
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versión de compilación técnica>_pt_br.exe
- KSMS_2_3_0_0.conf: archivo de configuración RBAC.
- KSMS_LegalNotices_en.txt: un archivo de texto con información sobre el código de terceros para Kaspersky Security Management Suite.
- Archivos del Contrato de licencia de usuario final de Kaspersky Security Management Suite:
 - eula_en_ksms_2.3.rtf
 - eula_es_ksms_2.3.rtf

- eula_pt_ksms_2.3.rtf
- eula_ru_ksms_2.3.rtf

Funcionamiento de Kaspersky Thin Client

El esquema de funcionamiento estándar de Kaspersky Thin Client (representado en la imagen de más abajo) puede diagramarse de este modo:

- Una vez instalado el sistema Kaspersky Thin Client en un cliente ligero, éste recibe los ajustes de red de un servidor DHCP o el administrador los configura manualmente.
- El administrador conecta y configura la interacción entre Kaspersky Thin Client y Kaspersky Security Center, y también instala el [complemento web](#) de Kaspersky Security Management Suite.
- Kaspersky Thin Client recibe los certificados de confianza, los ajustes de conexión al entorno remoto, la fecha y hora, y otros ajustes básicos mediante una [directiva](#) creada a través de Kaspersky Security Center Web Console.
- El usuario se conecta al [entorno remoto](#).
- En caso de problemas, el usuario envía [registros de auditoría y eventos](#) a través de la interfaz de Kaspersky Thin Client a un [servidor de registro de eventos](#) implementado en la infraestructura empresarial.
- El administrador [actualiza Kaspersky Thin Client](#).



Esquema de funcionamiento estándar de Kaspersky Thin Client

La siguiente imagen muestra un diagrama de la comunicación de Kaspersky Thin Client con plataformas de virtualización y entornos remotos.

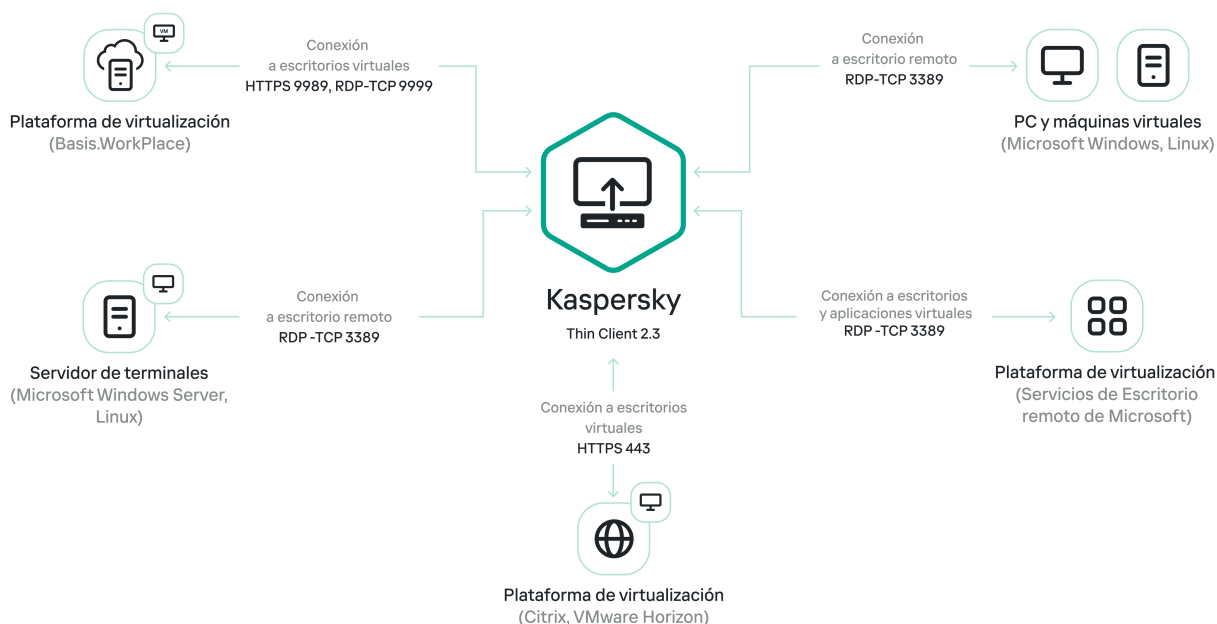


Diagrama de comunicación entre Kaspersky Thin Client y las plataformas de virtualización y entornos remotos

Requisitos de hardware y software

En esta sección, se describen los requisitos de hardware y software de Kaspersky Thin Client 2.3.

Este documento no incluye información sobre los componentes de hardware del cliente ligero, como controles y conectores, ya que estos detalles se encuentran en la documentación del vendedor del dispositivo donde está instalado Kaspersky Thin Client.

Requisitos del monitor

Kaspersky Thin Client permite conectar dos monitores.

Dependiendo de la configuración de orientación de la pantalla, Kaspersky Thin Client admite las siguientes resoluciones de monitor:

- Si la orientación de la pantalla está configurada en horizontal o en horizontal invertido:
 - 1024x768 (XGA)
 - 1280x720 (HD)
 - 1280x1024 (SXGA)
 - 1280x768 (WXGA)

- 1440x900 (WXGA+)
- 1400x1050 (SXGA+)
- 1920x1080 (Full HD)
- Si la orientación de la pantalla está configurada en vertical o vertical invertido:
 - 1280x1024 (SXGA)
 - 1400x1050 (SXGA+)
 - 1920x1080 (Full HD)

Kaspersky Thin Client admite las siguientes interfaces de conexión:

- HDMI
- DisplayPort

Kaspersky Thin Client solo es compatible con monitores de color verdadero.

Requisitos para periféricos conectados a Kaspersky Thin Client

Kaspersky Thin Client admite los siguientes dispositivos periféricos:

- Teclados y ratones USB sin funciones multimedia y teclados y ratones inalámbricos (radio).
- Unidades de memoria USB.
- Tarjetas inteligentes y tokens USB.
- Dispositivos de impresión y escaneo conectados por USB: impresoras, escáneres (incluidos escáneres de códigos QR y códigos de barras).
Se debe instalar un controlador (driver) para el dispositivo conectado al cliente ligero en el entorno remoto.
- Dispositivos de grabación y reproducción de audio con cables conectados a un mini-jack y a través de un puerto USB, y auriculares USB inalámbricos (radio).
- Cámaras web conectadas a través de un puerto USB.

Requisitos para sistemas de virtualización y acceso remoto

Kaspersky Thin Client admite los siguientes sistemas de virtualización y acceso remoto:

- Basis.WorkPlace 2.4.1
- Citrix Virtual Apps and Desktops 2402 cu1
Cliente: Aplicación Citrix Workspace para HTML5 24.11.0.51

Requisitos de red

La red debe permitir una velocidad de transmisión mínima de 50 Mb/s.

Requisitos para Kaspersky Security Center y Kaspersky Security Center Web Console

El sistema Kaspersky Thin Client es compatible con la versión 15.3 de Kaspersky Security Center Linux. Los requisitos de software y del sistema para el servidor en el que se instala Kaspersky Security Center se enumeran en la [guía de ayuda en línea de Kaspersky Security Center](#).

Requisitos para el servidor de registros

El [servidor de registros](#) debe cumplir con los siguientes requisitos:

- Kaspersky Thin Client se conecta al servidor de registros mediante HTTPS (de manera predeterminada, se usa el puerto 443).
- Kaspersky Thin Client se conecta al servidor de registros solo si existe un certificado de seguridad.
- Kaspersky Thin Client envía [los registros de eventos y de auditoría](#) al servidor de registros utilizando el método PUT.

Para obtener instrucciones sobre cómo instalar y configurar el servidor de registros, consulte la [Base de conocimientos](#).

Métodos de conexión remota

En esta sección, se brinda información sobre las tecnologías de conexión remota y los [entornos remotos](#) que son compatibles con Kaspersky Thin Client. También se enumeran las formas disponibles para conectarse a esos entornos mediante las aplicaciones de Kaspersky Thin Client.

Kaspersky Thin Client utiliza las siguientes aplicaciones:

- **RDP:** permite conectarse a escritorios remotos o aplicaciones virtuales a través del protocolo RDP.
- **Basis.WorkPlace:** permite conectarse a escritorios virtuales desplegados en una infraestructura Basis.WorkPlace.
- **Web Access:** conéctese a un entorno remoto implementado en una infraestructura de Citrix Workspace.

También se brinda información sobre los dispositivos conectados a Kaspersky Thin Client que se pueden redirigir a los entornos remotos.

Conexiones mediante la aplicación RDP

Puede utilizar Kaspersky Thin Client para conectarse mediante RDP a un entorno remoto (por ejemplo, a Servicios de Escritorio remoto de Microsoft [MS RDS]). En la siguiente tabla, se describen los métodos de conexión y los periféricos que se admiten para los sistemas operativos Windows y Linux.

A partir de la versión 2.3.4, Kaspersky Thin Client proporciona conexión en caliente de tokens USB, unidades de memoria USB e impresoras (USB) durante una sesión de conexión remota activa.

Si desea redirigir periféricos a un escritorio remoto que ejecute Linux, instale Kaspersky USB Redirector para el servidor xRDP en el sistema operativo invitado. Kaspersky USB Redirector no viene incluido en el kit de distribución. Puede solicitar esta extensión a Kaspersky.

Si desea ver instrucciones para conectarse a un entorno remoto, consulte [este otro artículo](#).

RDP: sistemas operativos, métodos de conexión y periféricos admitidos

	Windows Server 2016/2019/2022 en MS RDS	Windows 10/11	Windows Server 2016/2019/2022	ALT Linux 11 RED OS 8	Astra Linux SE 1.8.1
Conexión a una aplicación virtual	✓	✓	✓	—	—
Conexión a un escritorio remoto					
Conexión directa	—	✓	✓	✓	✓
Conexión mediante VDI	✓	—	—	—	—
Conexión de terminal	✓	—	✓	✓	✓
Periféricos					
Tokens USB	✓	✓	✓	✓ Nota	—
Tarjetas inteligentes (USB)	✓	✓	✓	✓ Nota	—
Unidades de memoria USB	✓	✓	✓	✓ Nota	—

Impresoras (USB)	✓	✓	✓ Nota ?	✓ Nota ?	—
Escáneres (USB)	✓	✓	✓ Nota ?	✓ Nota ?	—
Escáneres de códigos QR y de códigos de barras (USB)	✓	✓	✓	✓	✓
Micrófonos (con miniconector o USB) Nota ?	✓	✓	✓ Nota ?	✓ Nota ?	✓ Nota ?
Dispositivos de reproducción de audio (con miniconector o USB) Nota ?	✓	✓	✓ Nota ?	✓ Nota ?	✓ Nota ?
Cámara web (video, USB)	✓	✓	✓	—	—

Conexiones mediante la aplicación Basis.WorkPlace

Kaspersky Thin Client puede conectarse a un entorno remoto de Basis.WorkPlace. En la siguiente tabla, se describen los métodos de conexión y los periféricos que se admiten para los sistemas operativos Windows y Linux.

Si desea redireccionar periféricos a un escritorio remoto que ejecute Linux, instale Kaspersky USB Redirector para el servidor xRDP en el sistema operativo invitado. Kaspersky USB Redirector no viene incluido en el kit de distribución. Puede solicitar esta extensión a Kaspersky.

Si desea ver instrucciones para conectarse a un entorno remoto, consulte [este otro artículo](#).

Basis.WorkPlace: sistemas operativos, métodos de conexión y periféricos admitidos

	Windows 10/11	Windows Server 2016/2019/2022	RED OS 8 ALT Linux 11 Astra Linux SE 1.8.1
Conexión a un escritorio remoto			
Conexión directa ?	—	—	—
Conexión mediante VDI ?	✓	✓	✓
Conexión de terminal ?	—	✓	—
Periféricos			
Tokens USB	✓	✓	—
Tarjetas inteligentes (USB)	✓	✓	—
Unidades de memoria USB	✓	✓	—
Impresoras (USB)	✓	✓ Nota ?	—
Escáneres (USB)	✓	✓	—
Escáneres de códigos QR y de códigos de barras (USB)	✓	✓	—
Micrófonos (con miniconector o USB) Nota ?	✓	✓	✓
Dispositivos de reproducción de audio (con miniconector o USB) Nota ?	✓	✓	✓
Cámara web (video, USB)	—	—	—

Conexiones mediante la aplicación Web Access

En la aplicación Web Access, puede conectarse a un entorno remoto desplegado en infraestructuras Citrix Workspace. Web Access admite HTML5 y proporciona una conexión HTTPS segura al conectarse. En la siguiente tabla, se describen los métodos de conexión y los periféricos específicos que están disponibles para sistemas operativos Windows.

Para ver las instrucciones de conexión, consulte [este otro artículo](#).

Web Access: sistemas operativos, métodos de conexión y periféricos admitidos

	Microsoft Windows 10/11	Microsoft Windows Server 2016/2019/2022
Conexión a un escritorio remoto		
Conexión directa ^[?]	—	—
Conexión mediante VDI ^[?]	✓	✓
Conexión de terminal ^[?]	—	✓
Dispositivos periféricos (Citrix Workspace)		
Tokens USB	—	—
Tarjetas inteligentes (USB)	—	—
Unidades de memoria USB (FAT16 y FAT32, hasta 128 GB)	✓	✓
Impresoras (USB)	✓	✓
Escáneres (USB)	✓	✓
Escáneres de códigos QR y de códigos de barras (USB)	✓	✓
Micrófonos (con miniconector o USB)	✓	✓
Nota ^[?]		
Dispositivos de reproducción de audio (con miniconector o USB)	✓	✓
Nota ^[?]		
Cámara web (video, USB)	✓	✓

En la versión actual de Kaspersky Thin Client, no es posible conectarse a escritorios remotos que ejecuten Linux; tampoco puede usarse la aplicación Web Access para conectarse a aplicaciones virtuales.

Cuando se accede un entorno remoto desplegado en la infraestructura Citrix Workspace, no es posible redirigir a un mismo tiempo más de dos dispositivos USB.

Novedades

Kaspersky Thin Client versión 2.3 ofrece las siguientes mejoras y características nuevas:

- Redirección de los siguientes dispositivos a un entorno de virtualización Citrix mediante Web Access:
 - Unidades de memoria USB (a través de la asignación de unidades del cliente, Client Drive Mapping).
 - Auriculares USB.
 - Cámaras web.
 - Dispositivos de impresión y escaneo: impresoras, escáneres (incluidos códigos de barras y códigos QR).
- Redireccionar los siguientes dispositivos a un entorno remoto mediante RDP:
 - Auriculares USB.
 - Cámaras web.
 - Dispositivos de impresión y escaneo: impresoras, escáneres (incluidos códigos de barras y códigos QR).
- Se agregó la capacidad de seleccionar un dispositivo de reproducción y grabación de audio en el panel de conexión durante una sesión remota.
- Se agregó la capacidad de configurar los siguientes ajustes para conectarse a un escritorio remoto de cliente ligero a través de RDP:
 - Conexión del administrador al escritorio remoto del cliente ligero (automática, confirmación del usuario o denegada).
 - Mostrar al administrador la ventana de la sesión remota del usuario en ejecución: automáticamente, con confirmación del usuario o denegar.
- Soporte para conexión remota a un cliente ligero a través del protocolo RDP con autorización por nombre del dispositivo y contraseña.
- Ahora se admite bloquear la pantalla del cliente ligero desde una sesión remota activa.
- Se agregó soporte para el cliente ligero Dell Wyse 3040.
- Compatibilidad con firmware UEFI, que aumenta la velocidad de arranque del cliente ligero y admite grandes cantidades de memoria.
- Se agregó la capacidad de mostrar en el escritorio del cliente ligero solo las aplicaciones que el usuario haya seleccionado en la configuración (RDP, Basis.WorkPlace o Web Access).
- Se agregó la capacidad de iniciar automáticamente una de las aplicaciones (RDP, Basis.WorkPlace o Web Access) según lo seleccionado por el usuario, al iniciar el cliente ligero.
- Se agregó la capacidad de conectarse automáticamente a un entorno remoto después de iniciar RDP.
- Se agregó un asistente de selección de idioma para la configuración inicial de Kaspersky Thin Client.

- Se agregó la capacidad de establecer un fondo personalizado en el escritorio de Kaspersky Thin Client a través de Kaspersky Security Center Web Console.
- Se agregó la capacidad de configurar una pantalla de inicio de personalizada en la pantalla de bloqueo de Kaspersky Thin Client a través de Kaspersky Security Center Web Console.
- Se agregó la capacidad de configurar monitores de manera centralizada a través de Kaspersky Security Center Web Console, incluidos los siguientes ajustes:
 - Resolución y orientación de la pantalla.
 - Modo de pantalla (escritorio duplicado o extendido) de la pantalla secundaria.
- Se agregó la capacidad de definir manualmente el tipo de un dispositivo conectado que el sistema no pueda reconocer.
- Ahora se puede redireccionar un auricular, teclado o mouse USB inalámbricos (por radio) a un entorno remoto.
- Se agregó compatibilidad con los siguientes idiomas de entrada: alemán (de-DE), francés de Suiza (fr-CH) y alemán de Suiza (de-CH).
- Se agregó la capacidad de anclar u ocultar completamente el panel de conexión en un entorno remoto.
- Se agregó la capacidad de [redireccionar](#) los siguientes tokens a través de RDP a un escritorio remoto de RED OS 8.0 y luego a un escritorio remoto de Windows 10, siempre que se haya iniciado una sesión de escritorio remoto entre estos escritorios:
 - Rutoken Lite
 - JaCarta-2 PKI / GOST
- Compatibilidad con la nueva versión de [Kaspersky Security Center Web Console](#), 15.3.
- Se ha mejorado el diseño y texto de la interfaz de usuario de Kaspersky Thin Client y [Kaspersky Security Management Suite](#).

Instalar y actualizar Kaspersky Thin Client

El procedimiento de instalación de Kaspersky Thin Client depende del [formato de entrega](#):

- Un socio entrega una plataforma de hardware con Kaspersky Thin Client preinstalado. En ese caso, la instalación de Kaspersky Thin Client en la plataforma de hardware la realiza TONK.
- Kaspersky Thin Client se entrega sin una plataforma de hardware (cliente ligero). En ese caso, la plataforma de software se instala siguiendo las instrucciones contenidas en esta sección.

Instalar Kaspersky Thin Client

Antes de instalar Kaspersky Thin Client, haga lo siguiente:

1. Prepare una unidad de memoria USB de arranque que contenga el sistema operativo Ubuntu Linux (versión recomendada: Ubuntu 20.04).
2. Copie los archivos de instalación de Kaspersky Thin Client [del kit de distribución](#) a una partición independiente en la unidad USB de arranque o a otra una unidad de memoria USB:
 - `Kaspersky_Thin_Client_<número de versión>_Wyse3040.tar.gz` o `Kaspersky_Thin_Client_<número de versión>_TN1200.tar.gz`: imagen de instalación.
 - `hw_install.sh`: script de instalación de Kaspersky Thin Client.

Para garantizar la seguridad antes de la instalación de Kaspersky Thin Client, recomendamos que actualice la BIOS del cliente ligero a la versión más reciente, que defina una contraseña para impedir cambios en la configuración de la BIOS y que habilite la opción para limitar el arranque al dispositivo SSD local. Estas recomendaciones ayudan a evitar determinados riesgos de seguridad, como la sustitución del sistema operativo, el reemplazo o la eliminación de los certificados de conexión a servidores remotos y el acceso no autorizado a los ajustes del sistema operativo.

Kaspersky Thin Client es compatible con la tecnología Secure Boot, que permite que el UEFI verifique la autenticidad de los componentes cargados. Si desea configurar Secure Boot, puede obtener las claves necesarias de los expertos de Kaspersky y seguir las instrucciones de la [Base de conocimientos](#).

Para instalar Kaspersky Thin Client en un cliente ligero:

1. Conecte la unidad USB de arranque preparada al [puerto correspondiente](#) del cliente ligero.
2. [Encienda el cliente ligero](#) e inicie la imagen de Ubuntu de la unidad USB de arranque. No instale el sistema en el disco duro del cliente ligero.
3. Cuando se cargue el sistema operativo, vaya al directorio con los archivos de instalación de Kaspersky Thin Client.
4. Ejecute el siguiente comando:

```
sudo bash ./hw_install.sh -u Kaspersky_Thin_Client_<número de versión>_<nombre de la
plataforma>.tar.gz
```

donde:

- `./hw_install.sh`: ruta al script de instalación.
- `Kaspersky_Thin_Client_<número de versión>_<nombre de la plataforma>.tar.gz`: imagen de instalación.

Si la instalación concluye sin errores, aparecerá el mensaje *Installed OK! Remove USB drive and reboot*.

5. Apague el cliente ligero y desconecte la unidad USB de arranque.

Cuando vuelva a encender el cliente ligero, se cargará el sistema Kaspersky Thin Client.

Puede consultar el número de versión del sistema operativo instalado en la [interfaz de Kaspersky Thin Client](#).

Actualizar Kaspersky Thin Client

Puede actualizar Kaspersky Thin Client de la versión 2.0 o 2.0.1 a la versión 2.3.

Antes de actualizar Kaspersky Thin Client, haga lo siguiente:

1. Prepare una unidad de memoria USB de arranque que contenga la distribución de Linux. Recomendamos utilizar Linux Ubuntu (versión recomendada: Ubuntu 20.04).
2. Asegúrese de que la utilidad OpenSSL esté instalada en el sistema. Si no está instalada, instálela iniciando el siguiente comando:

```
sudo apt install openssl
```

3. Copie los siguientes archivos del kit de distribución de Kaspersky Thin Client 2.3 en un directorio de la unidad de memoria USB:

- Archivo que contiene la imagen de instalación `Kaspersky_Thin_Client_<número de versión>_TN1200.tar.gz`.
- Scripts de instalación y actualización:
 - `hw_install.sh`
 - `hw_update.sh`
 - `save_files.sh`
 - `restore_files.sh`

Para actualizar Kaspersky Thin Client en un cliente ligero:

1. Conecte la unidad USB de arranque preparada al puerto correspondiente del cliente ligero.
2. [Encienda el cliente ligero](#) y ejecute la imagen de Ubuntu de la unidad USB de arranque. No instale el sistema en el disco duro del cliente ligero. Para hacerlo, seleccione la opción *Try without installation*.

3. En el sistema operativo en ejecución, vaya al directorio que contiene los scripts y la imagen de instalación de Kaspersky Thin Client 2.3.

4. Inicie el script de actualización utilizando el siguiente comando:

```
sudo bash ./hw_update.sh -u <ruta al archivo comprimido que contiene la imagen de
instalación de Kaspersky Thin Client>
```

Si el script de actualización se completó correctamente, aparecerá el mensaje *Updated OK!*

Si se produjo un error mientras se iniciaba el script, [comuníquese con el Soporte técnico](#).

5. Apague el cliente ligero y desconecte la unidad USB de arranque.

La actualización queda instalada. La siguiente vez que encienda el dispositivo, podrá utilizar Kaspersky Thin Client 2.3.

Interfaz de Kaspersky Thin Client

La interfaz de Kaspersky Thin Client consta de los siguientes elementos:

- Escritorio con aplicaciones.
- Panel de control en la parte superior de la ventana.
- Panel de conexión que se muestra durante una sesión remota.

Escritorio

La parte central del escritorio de Kaspersky Thin Client muestra las aplicaciones que puede usar para conectarse a un [entorno remoto](#) .

- **RDP**: conéctese a escritorios remotos o aplicaciones virtuales a través del protocolo RDP.
- **Basis.WorkPlace**: conéctese a escritorios virtuales desplegados en la infraestructura Basis.WorkPlace.
- **Web Access**: conéctese a un entorno remoto implementado en una infraestructura de Citrix Workspace.

Panel de control

El panel de control de Kaspersky Thin Client consta de los siguientes elementos:

-  es un botón para llamar el menú de apagado.
Utilice este menú para [apagar](#) o [reiniciar](#) Kaspersky Thin Client.
-  es un botón para abrir las secciones **Ajustes** y **Herramientas**:
Use la sección **Ajustes** para [configurar Kaspersky Thin Client](#).
Use la sección **Herramientas** para lo siguiente:
 - [Ver información sobre Kaspersky Thin Client](#).
 - [Ver información sobre el estado de la red](#).
 - [Ver y transmitir los registros de eventos de Kaspersky Thin Client](#).
 - Ver información sobre las actualizaciones de Kaspersky Thin Client.
 - [Ver el Contrato de licencia de usuario final actual](#).
 - [Ver información sobre código de terceros](#).
 - [Configurar el acceso a los ajustes de Kaspersky Thin Client](#).
-  es un botón para abrir la ventana que contiene [información sobre el cliente ligero y los Contactos del Servicio de soporte técnico](#).
- [Estado de la conexión de red de Kaspersky Thin Client](#) .

-  es un botón para abrir el [panel de notificaciones](#).
- Botón para [cambiar el idioma de entrada](#) del teclado.
- [Fecha y hora del sistema](#).
-  es un botón para abrir el menú de [administración remota de Kaspersky Thin Client](#).

Panel de conexión

El [panel de conexión](#) se muestra durante una [sesión remota](#) .

Cuando el dispositivo está conectado a un escritorio remoto, el panel de conexión muestra los siguientes datos y elementos:

-  es un botón para [cerrar una sesión remota](#).
- Nombre de la conexión.
- Estado de la conexión.
-  es un botón para abrir la ventana que contiene [información sobre el cliente ligero y los Contactos del Servicio de soporte técnico](#).
-  es un botón para [bloquear una sesión remota](#).
-  es un botón para abrir el [panel de notificaciones](#).
- Icono de estado de la red.
-  es un botón para abrir la ventana para [administrar los dispositivos de reproducción y grabación de audio](#).
El botón se muestra si dos o más dispositivos de este tipo están conectados al cliente ligero.
-  es un botón para abrir la ventana para [administrar la redirección de dispositivos USB](#).
El botón se muestra [al conectarse a un entorno remoto implementado en una infraestructura de Citrix Workspace](#).

Cuando el dispositivo está conectado a una aplicación virtual, el panel de conexión muestra también los siguientes elementos:

- Ícono de la aplicación.
- Fecha actual configurada en Kaspersky Thin Client.
- Hora actual configurada en Kaspersky Thin Client.
- Idioma en que se muestra la interfaz de Kaspersky Thin Client.

Licencia de Kaspersky Thin Client

Los términos de uso de Kaspersky Thin Client están estipulados en el Contrato de licencia de usuario final o en un documento similar que regule el uso de la aplicación.

El *Contrato de licencia de usuario final* es un contrato legalmente vinculante, celebrado entre usted y AO Kaspersky Lab, en el que se estipulan los términos bajo los cuales puede usar Kaspersky Thin Client.

Lea atentamente los términos y condiciones del Contrato de licencia de usuario final antes de comenzar a utilizar Kaspersky Thin Client.

Usted aceptará los términos y condiciones del Contrato de licencia de usuario final cuando, al iniciarse el sistema por primera vez, confirme estar de acuerdo con el texto del Contrato de licencia de usuario final. Si no acepta los términos y condiciones del Contrato de licencia de usuario final, cancele el inicio de Kaspersky Thin Client y no lo utilice. Cuando [Kaspersky Thin Client se actualiza](#), los cambios que pudiera haber en los términos y condiciones del Contrato de licencia de usuario final para la nueva versión de Kaspersky Thin Client son aceptados por el administrador de Kaspersky Security Center.

Si es necesario, puede ver el texto del Contrato de licencia de usuario final en la interfaz de Kaspersky Thin Client.

Para ver el texto del Contrato de licencia de usuario final,

en el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Herramientas → Contrato de licencia de usuario final**.

Se abre una ventana con el texto del Contrato de licencia de usuario final asociado a la versión de Kaspersky Thin Client instalada.

Provisión de datos

Kaspersky Thin Client no transmite datos de ningún tipo a Kaspersky. Los datos se procesan en los [clientes ligeros](#) en los que se encuentra instalado Kaspersky Thin Client y en los servidores de la infraestructura local que interactúan con Kaspersky Thin Client.

Kaspersky Thin Client guarda la siguiente información en el cliente ligero:

- Un [registro de eventos](#), con datos técnicos sobre el funcionamiento del sistema e información sobre los eventos de Kaspersky Thin Client enviados al Servidor de administración de Kaspersky Security Center.
- [Registro de auditoría](#) que contiene los siguientes eventos y sus detalles:
 - Agregar, reemplazar y cambiar certificados para conectarse a Kaspersky Security Center en la interfaz de Kaspersky Thin Client.
 - Restablecimiento de los ajustes de Kaspersky Thin Client.
 - Aceptar una conexión remota al cliente ligero.
 - Crear un nuevo archivo de registro de auditoría en caso de rotación de registros.
 - Guardar y eliminar la contraseña de usuario para la conexión automática a un entorno remoto.
 - Habilitar (manual y automáticamente) y deshabilitar la administración de Kaspersky Thin Client a través de Kaspersky Security Center.
- Ajustes del sistema:
 - Fecha y hora en que se realizó la instalación de Kaspersky Thin Client en el cliente ligero.
 - Nombre del cliente ligero.
 - Versión de Kaspersky Thin Client que se encuentra instalada.
 - Idioma en que se muestra la interfaz de Kaspersky Thin Client.
 - Lista de idiomas disponibles cuando se cambia el idioma de entrada del teclado.
 - Ubicación (coordenadas) del panel de conexión.
 - Hora de la última ocasión en que se usaron certificados para autenticarse al establecer conexión con agentes, con escritorios remotos o aplicaciones virtuales a través de RDP, con escritorios remotos de Basis.WorkPlace, con entornos remotos en Web Access o con un servidor de registros.
 - Dispositivo de grabación y reproducción de sonido seleccionado como principal.
 - Lista de aplicaciones que se muestran en el escritorio de Kaspersky Thin Client.
 - Aplicación seleccionada por el usuario para iniciarse automáticamente.
 - Lista de dispositivos USB no identificados cuyo tipo se define manualmente.

- Archivos de fondo de pantalla y de pantalla de bloqueo instalados en el cliente ligero, junto con sus metadatos.
- Configuración de los monitores conectados:
 - Monitores principal y secundario.
 - Id. de los monitores principal y secundario.
 - Resolución de los monitores principal y secundario.
 - Orientación de los monitores principal y secundario.
 - Modo de pantalla para un monitor secundario.
- Ajustes de interacción con Kaspersky Security Center:
 - Dirección (nombre o dirección IP y puerto) del Servidor de administración de Kaspersky Security Center.
 - Método de conexión a Kaspersky Security Center (manual o con DHCP).
 - Conjunto de identificadores de Kaspersky Thin Client para establecer conexión con Kaspersky Security Center.
 - Período de sincronización entre Kaspersky Thin Client y Kaspersky Security Center (expresado en minutos).
 - Cantidad de certificados recibidos de Kaspersky Security Center para autenticar las conexiones de Kaspersky Thin Client con los distintos agentes, con escritorios remotos o aplicaciones virtuales a través de RDP, con escritorios remotos de Basis.WorkPlace, con entornos remotos en Web Access o con un servidor de registros.
 - Huella digital del certificado utilizado para autenticar la conexión de Kaspersky Thin Client con Kaspersky Security Center.
 - Patrón de denominación definido por el administrador de Kaspersky Security Center para los clientes ligeros (nombre, id. y detalles adicionales de los clientes ligeros).
 - Conjunto de secretos para confirmar las acciones del usuario (el restablecimiento de la configuración y de los datos, la desconexión del cliente ligero de Kaspersky Security Center y la sustitución del certificado utilizado para conectar el cliente ligero a Kaspersky Security Center) en la interfaz de Kaspersky Thin Client.
 - Datos de contacto del servicio de soporte técnico.
 - Archivos de los certificados para autenticar la conexión de Kaspersky Thin Client con Kaspersky Security Center.
- Ajustes de conexión de Web Access:
 - Dirección web del servidor.
 - Archivos de los certificados utilizados para autenticar las conexiones.
 - Datos que se necesiten para usar el entorno remoto (por ejemplo, cookies).

- Ajustes de conexión a Basis.WorkPlace:
 - Dirección (nombre o dirección IP y puerto) del administrador de conexiones de Basis.WorkPlace.
 - Nombre de usuario para conectarse al administrador de conexiones de Basis.WorkPlace.
 - Archivos de los certificados para autenticar el agente al conectarse a un escritorio remoto administrado por Basis.WorkPlace.
 - Id. de Kaspersky Thin Client.
 - Número de intentos de reconexión.
 - Perfil de la conexión disponible entre Kaspersky Thin Client y el agente de Basis.WorkPlace.
 - Ajustes para la redirección de periféricos al escritorio remoto: habilitación o deshabilitación de la redirección de tarjetas inteligentes y unidades de memoria USB.
 - Indicación de si el uso de dos monitores está habilitado o deshabilitado.
 - Lista de direcciones (nombre o dirección IP y puerto) de los administradores de conexiones de una instalación geodistribuida administrada por Basis.WorkPlace.
- Ajustes de conexión al servidor RDP:
 - Dirección (nombre o dirección IP y puerto) del servidor del Agente de conexión a Escritorio remoto.
 - Dominio y nombre de usuario para conectarse al servidor del Agente de conexión a Escritorio remoto.
 - Id. de colección del Agente de conexión a Escritorio remoto.
 - Alias de la aplicación.
 - Archivos de los certificados para autenticar el servidor del Agente de conexión a Escritorio remoto al conectarse a un escritorio remoto o a una aplicación virtual a través de RDP.
 - Ajustes para la redirección de periféricos al escritorio remoto:
 - Si la redirección de unidades USB está activada o desactivada.
 - Si la redirección de tarjetas inteligentes está activada o desactivada.
 - Indicación de si la redirección de impresoras está habilitada o deshabilitada.
 - Indicación de si la redirección de dispositivos de reproducción de audio está habilitada o deshabilitada.
 - Indicación de si la redirección de dispositivos de grabación de audio está habilitada o deshabilitada.
 - Indicación de si la redirección de la transmisión de video de la cámara web está permitida.
 - Indicación de si la redirección de escáneres está habilitada o deshabilitada.
 - Indicación de si el uso de dos monitores está habilitado o deshabilitado.

- Indicación de si se encuentra habilitada o deshabilitada la conexión automática al escritorio remoto o a la aplicación virtual tras una desconexión inesperada.
- Ajustes de calidad de la imagen:
 - Indicación de si el suavizado de fuentes está habilitado o deshabilitado.
 - Indicación de si los menús animados están habilitados o deshabilitados.
 - Indicación de si se muestra el fondo de escritorio.
 - Indicación de si se muestra el contenido de las ventanas cuando se las arrastra.
 - Indicación de si los temas de Microsoft Windows están habilitados o deshabilitados.
- Indicación de si se encuentra habilitada o deshabilitada la conexión automática al escritorio remoto:
 - Contraseña para conectarse al escritorio remoto, solo si se selecciona la opción de conexión automática.
- Ajustes de la conexión RDP del cliente ligero:
 - Certificado de servidor RDP.
 - Secreto.
 - Modo de conexión de escritorio remoto de cliente ligero (conexión automática, confirmación del usuario o denegada).
 - Modo de pantalla del contenido remoto (automático, confirmación del usuario o deshabilitado).
- Ajustes de la red:
 - Indicación de si se encuentra habilitado o deshabilitado el uso de DHCP para configurar la red en forma automática.
 - Dirección IP del cliente ligero.
 - Máscara de subred.
 - Lista de direcciones IP de los servidores DNS.
 - Dirección IP de la puerta de enlace de la red.
- Ajustes de ahorro de energía: cantidad de minutos que se dejan transcurrir antes de apagar el monitor y cantidad de minutos que se dejan transcurrir antes de apagar el cliente ligero cuando Kaspersky Thin Client queda inactivo.
- Ajustes de conexión al servidor de registros:
 - Dirección (nombre o dirección IP y puerto) del servidor de registros al que se envían los registros de eventos y de auditoría.
 - Archivos de los certificados para autenticar el servidor de registros cuando Kaspersky Thin Client se conecta a dicho servidor.

- Ajustes de fecha y hora:
 - Fecha y hora recibidas del Servidor de administración durante la última sincronización con Kaspersky Security Center.
 - Zona horaria.
- Información sobre las actualizaciones de Kaspersky Thin Client disponibles y descargadas:
 - Estado de disponibilidad de las actualizaciones.
 - Estado de instalación de las actualizaciones.
 - Estado de entrega de las actualizaciones.
 - Datos de la actualización disponible: versión de Kaspersky Thin Client, nombre de la versión, fecha y hora, importancia.
 - Hora de la última búsqueda de actualizaciones llevada a cabo correctamente.
 - Hora de la última instalación de actualizaciones llevada a cabo correctamente.
- Información sobre los contratos de licencia de usuario final de Kaspersky Thin Client:
 - Identificadores de los contratos de licencia de usuario final.
 - Contratos de licencia de usuario final en ruso, inglés, español y portugués de Brasil.
 - Información sobre si se aceptaron o no los contratos de licencia de usuario final.
 - Información sobre las fechas de publicación de los contratos de licencia de usuario final.

Kaspersky protege la totalidad de la información recibida de conformidad con los requisitos establecidos por la ley y con arreglo a las regulaciones vigentes de Kaspersky. Los datos se transmiten a través de canales de comunicación cifrados.

Encender e iniciar Kaspersky Thin Client por primera vez

Antes de utilizar Kaspersky Thin Client, conecte un mouse, un teclado y un monitor al cliente ligero a través de los puertos correspondientes. Kaspersky Thin Client también permite conectar [periféricos](#) mientras el sistema está en funcionamiento.

Este documento no contiene una descripción general de los controles, conectores y demás componentes de hardware que conforman los clientes ligeros; si necesita esta información, la encontrará en la documentación ofrecida por el proveedor de su dispositivo. Para conocer los modelos de cliente ligero específicos en los que se puede instalar Kaspersky Thin Client, consulte [la sección con información básica sobre Kaspersky Thin Client](#).

Para comenzar a trabajar con Kaspersky Thin Client, encienda el cliente ligero.

Para encender Kaspersky Thin Client y completar el procedimiento de primer inicio:

1. Presione el botón de encendido/apagado del cliente ligero.

Kaspersky Thin Client comenzará a cargarse en su dispositivo. Una vez cargado el sistema, aparece la ventana de selección de idioma de la interfaz de usuario.

2. Seleccione el idioma que desee usar para la interfaz y haga clic en **Siguiente**.

Se abrirá una ventana con el texto del [Contrato de licencia de usuario final](#) en el idioma que haya seleccionado.

3. Lea atentamente el texto del Contrato de licencia de usuario final y haga clic en **Aceptar**.

Si no acepta los términos y condiciones del Contrato de licencia de usuario final, cancele el inicio de Kaspersky Thin Client y no lo utilice.

En este punto, habrá concluido el lanzamiento inicial. Se mostrará el [escritorio](#) de Kaspersky Thin Client.

El escritorio aparecerá cada vez que se cargue el sistema tras encender el cliente ligero.

Reiniciar y apagar Kaspersky Thin Client

Cada vez que termine de trabajar con Kaspersky Thin Client, apague el cliente ligero.

Para apagar Kaspersky Thin Client:

1. En el escritorio de Kaspersky Thin Client, dentro del panel de control, haga clic en el botón de apagado, .
2. En el menú que se abre, haga clic en **Apagar**.

Kaspersky Thin Client se apagará.

Puede reiniciar Kaspersky Thin Client si resulta necesario. Esto puede suceder, por ejemplo, cuando se desea aplicar el nuevo idioma seleccionado a la interfaz de Kaspersky Thin Client o cuando se debe instalar un conjunto de actualizaciones en el sistema.

Para reiniciar Kaspersky Thin Client:

1. En el escritorio de Kaspersky Thin Client, dentro del panel de control, haga clic en el botón de apagado, .
2. En el menú que se abre, seleccione **Reiniciar**.

Kaspersky Thin Client se reiniciará.

Uso de certificados en Kaspersky Thin Client

El [protocolo de cifrado TLS](#) garantiza la transferencia de datos segura entre un cliente y un servidor mediante el uso de certificados de conexión SSL. Un *certificado de conexión SSL* (en adelante, "certificado SSL" o simplemente "certificado") es un bloque de datos que contiene información sobre el titular de dicho certificado, la clave pública del titular y las fechas en que comienza y termina la vigencia del certificado.

En Kaspersky Thin Client, los certificados se utilizan para estos fines:

- [Conexión de un cliente ligero a Kaspersky Security Center](#).
- Conexión a un entorno remoto:
 - Autenticación del Agente de conexión a Escritorio remoto al conectarse a un escritorio remoto o a una aplicación virtual.
 - Autenticación del agente al conectarse a un escritorio remoto administrado por Basis.WorkPlace.
 - Autenticación de la dirección del servidor al conectarse a un entorno remoto en Web Access.
- Conexión a un servidor de registros.

El usuario puede [aceptar o rechazar un certificado de forma independiente en la interfaz de Kaspersky Thin Client](#) si se cumplen las siguientes condiciones:

- El usuario se está conectando a un [entorno remoto](#) o a un [servidor de registro](#) en la interfaz de Kaspersky Thin Client por primera vez.
- El cliente ligero se encuentra en uno de los siguientes estados:
 - No conectado a Kaspersky Security Center.
 - No agregado al grupo de administración.
 - [No se han agregado certificados para conectarse al entorno remoto](#) para el grupo de administración al que pertenece el cliente ligero.

Los certificados aceptados se guardan en el almacén de certificados del cliente ligero. En este caso, el usuario también puede conectarse a nodos y usar certificados que no estén controlados por el administrador.

Le recomendamos [configurar la conexión de un grupo de clientes ligeros](#) a un servidor de registros o a un entorno remoto utilizando únicamente los certificados asignados por el administrador en Web Console. En tal caso, todos los certificados aceptados por el usuario se eliminarán del almacén de certificados del cliente ligero. Estas medidas ayudará a evitar que Kaspersky Thin Client se conecte a nodos que no sean de confianza.

Le recomendamos actualizar los certificados asignados en los siguientes casos:

- Los certificados utilizados se ven comprometidos.
- Los certificados caducan.
- Los certificados tienen que actualizarse periódicamente porque la empresa así lo exige en su política para la seguridad de la información.

Kaspersky Thin Client no verifica si los certificados están en la lista de revocación de certificados.

Configurar Kaspersky Thin Client

En esta sección, encontrará información para configurar Kaspersky Thin Client.

Procedimiento: inicio rápido para administradores

En esta sección, se describe la secuencia de pasos que debe realizar para configurar Kaspersky Thin Client y Kaspersky Security Center, así como para establecer una conexión entre estas dos soluciones. Estos pasos deben los debe ejecutar el administrador u otro experto calificado de su organización que pueda verificar la autenticidad del certificado aceptado utilizado para conectarse a Kaspersky Security Center.

Si desea obtener instrucciones para instalar Kaspersky Thin Client en un cliente ligero, consulte [este otro artículo](#).

Antes de instalar Kaspersky Thin Client o de iniciar por primera vez un cliente ligero que traiga un sistema Kaspersky Thin Client preinstalado, tenga a bien actualizar la BIOS del cliente ligero a la versión más reciente, defina una contraseña para evitar cambios en la configuración de la BIOS y habilite la opción para limitar el arranque al dispositivo SSD local. Estas recomendaciones ayudan a evitar determinados riesgos de seguridad, como la sustitución del sistema operativo, el reemplazo o la eliminación de los certificados de conexión a servidores remotos y el acceso no autorizado a los ajustes del sistema operativo.

Kaspersky Thin Client es compatible con la tecnología Secure Boot, que permite que el UEFI verifique la autenticidad de los componentes cargados. Si desea configurar Secure Boot, puede obtener las claves necesarias de los expertos de Kaspersky y seguir las instrucciones de la [Base de conocimientos](#).

El procedimiento para realizar la configuración inicial de Kaspersky Thin Client y Kaspersky Security Center y conectar estas soluciones se divide en los siguientes pasos:

1 Instalar Kaspersky Security Center

Descargue el paquete de distribución de Kaspersky Security Center e instale la versión completa de Kaspersky Security Center en el servidor. El paquete de distribución de la versión completa de Kaspersky Security Center incluye Kaspersky Security Center Web Console. Recomendamos seleccionar el modo de instalación estándar. Para obtener más información sobre la instalación de Kaspersky Security Center, consulte la [Ayuda en línea de Kaspersky Security Center](#).

2 Configurar las reglas del firewall

Si piensa usar el puerto predeterminado para conectar el cliente ligero a Kaspersky Security Center, en el sistema operativo del servidor en el que esté instalado Kaspersky Security Center, cree reglas para que el firewall permita las conexiones TCP a través del puerto 13292. Si desea usar un puerto que no sea el 13292, configure los permisos correspondientes. Para obtener información detallada sobre cómo configurar las reglas del firewall, consulte la documentación de su sistema operativo.

3 Instalar el complemento web de Kaspersky Security Management Suite

En Kaspersky Security Center Web Console, instale el [complemento web Kaspersky Security Management Suite](#).

4 Preparar los puertos

Kaspersky Thin Client utiliza un protocolo móvil para conectarse con Kaspersky Security Center. En el Servidor de administración de Kaspersky Security Center, habilite el uso del puerto TCP al que permitió el acceso en el paso 2. Para obtener más información sobre cómo habilitar un puerto TCP en el Servidor de administración de Kaspersky Security Center, consulte la [Ayuda en línea de Kaspersky Security Center](#).

5 Encender Kaspersky Thin Client

[Encienda Kaspersky Thin Client](#) y espere a que se cargue el sistema. Seleccione el idioma del sistema. Lea los términos y condiciones del contrato de licencia de usuario final y acepte el contrato.

6 Configurar los ajustes de Kaspersky Thin Client

Después de encender Kaspersky Thin Client y aceptar el contrato de licencia de usuario final, configure los [ajustes generales](#) y los [ajustes de conexión a la red](#).

7 Configurar la conexión entre Kaspersky Thin Client y Kaspersky Security Center

En la interfaz de Kaspersky Thin Client, [configure la conexión a Kaspersky Security Center](#).

8 Cómo agregar un cliente ligero con Kaspersky Thin Client a un grupo de administración

En la consola web, [agregue el cliente ligero al grupo de administración](#) manualmente o configure la transferencia automatizada de dispositivos.

9 Crear una directiva activa en Kaspersky Security Center

En la interfaz de Web Console, [cree una directiva activa](#) para el grupo de administración.

10 Asignar certificados a un grupo de administración

[Asigne los certificados necesarios](#) para conectar un grupo de administración a un entorno remoto y a un servidor de registros. Recomendamos que también [agregue un certificado de reserva](#) para la conexión entre Kaspersky Thin Client y Kaspersky Security Center.

Una vez que complete estas acciones, el sistema Kaspersky Thin Client estará listo para funcionar. Podrá controlar Kaspersky Thin Client mediante la interfaz de Kaspersky Thin Client o a través de Kaspersky Security Center Web Console. También podrá monitorear los eventos de Kaspersky Thin Client.

Procedimiento: asignar certificados a un grupo de clientes ligeros

Si utiliza Kaspersky Security Center Web Console para asignar certificados para un [grupo de administración](#), los usuarios de los clientes ligeros incluidos en ese grupo solo podrán conectarse a los servidores para los que se hayan agregado certificados en Web Console.

[Kaspersky Security Center debe instalarse y configurarse](#) de antemano.

El procedimiento para asignar certificados para un grupo de clientes ligeros consta de los siguientes pasos:

1 Configurar la conexión a Kaspersky Security Center

En la interfaz de Kaspersky Thin Client, [configure la conexión a Kaspersky Security Center](#).

2 Agregar clientes ligeros al grupo de administración

En la interfaz de Web Console, si tiene algún cliente ligero que aún esté en el grupo de dispositivos no asignados, [agréguelo al grupo de administración](#).

3 Crear una directiva activa de Kaspersky Security Center para Kaspersky Thin Client

En la interfaz de Web Console, [cree una directiva activa](#) para el grupo de administración en cuestión.

4 Agregar los certificados para conectarse a un entorno remoto y a un servidor de registros

En la interfaz de Kaspersky Security Center Web Console, [agregue los certificados pertinentes](#) y ponga el interruptor ubicado en la parte derecha de la página en la posición **Imponer**. Espere a que Kaspersky Thin Client se sincronice completamente con Kaspersky Security Center. Puede definir el período de sincronización al configurar Kaspersky Thin Client a través de Kaspersky Security Center Web Console. Cuando se complete la sincronización, los dispositivos recibirán los certificados del Servidor de administración de Kaspersky Security Center.

Si [elimina todos los certificados](#) asignados a un grupo de dispositivos, quienes usen los clientes ligeros pertenecientes a ese grupo de dispositivos podrán conectarse a cualquier servidor, incluidos los servidores a los que no se les haya asignado ningún certificado.

Procedimiento: migrar clientes ligeros a un nuevo servidor de Kaspersky Security Center

En esta sección se describen los pasos que debe realizar el administrador al configurar los dispositivos que ejecutan Kaspersky Thin Client para administrarlos a través de un nuevo Servidor de administración de Kaspersky Security Center (en adelante, también denominado "el Servidor") si estos dispositivos se administraban a través de otro servidor de Kaspersky Security Center.

Para configurar la administración de Kaspersky Thin Client si los clientes ligeros se van a migrar a un nuevo servidor de Kaspersky Security Center, siga estos pasos:

1 Instalar un nuevo Servidor de administración de Kaspersky Security Center

Descargue el paquete de distribución de Kaspersky Security Center e instale la versión completa de Kaspersky Security Center en el servidor. El paquete de distribución de la versión completa de Kaspersky Security Center incluye Kaspersky Security Center Web Console. Recomendamos seleccionar el modo de instalación estándar. Para obtener más información sobre la instalación de Kaspersky Security Center, consulte la [Ayuda en línea de Kaspersky Security Center](#).

2 Configurar las reglas del firewall

Si piensa usar el puerto predeterminado para conectar el cliente ligero a Kaspersky Security Center, en el sistema operativo del servidor en el que esté instalado Kaspersky Security Center, cree reglas para que el firewall permita las conexiones TCP a través del puerto 13292. Si desea usar un puerto que no sea el 13292, configure los permisos correspondientes. Para obtener información detallada sobre cómo configurar las reglas del firewall, consulte la documentación de su sistema operativo.

3 Instalar el complemento web de Kaspersky Security Management Suite

En Web Console, instale el [complemento web de Kaspersky Security Management Suite](#) para el nuevo Servidor de administración de Kaspersky Security Center.

4 Preparar los puertos

Kaspersky Thin Client utiliza un protocolo móvil para conectarse con Kaspersky Security Center. En el Servidor de administración de Kaspersky Security Center, habilite el uso del puerto TCP al que permitió el acceso en el paso 2. Para obtener más información sobre cómo habilitar un puerto TCP en el Servidor de administración de Kaspersky Security Center, consulte la [Ayuda en línea de Kaspersky Security Center](#).

5 Encender Kaspersky Thin Client

[Encienda Kaspersky Thin Client](#) y espere a que se cargue el sistema.

6 Crear una directiva activa de Kaspersky Security Center para Kaspersky Thin Client

En la instancia antigua de Web Console, [cree una directiva activa para el grupo de dispositivos](#) que planee administrar con el nuevo servidor de Kaspersky Security Center.

7 Actualizar el certificado de seguridad para conectarse a Kaspersky Security Center

[Emita un certificado](#), que tenga que ser guardado en el Servidor de administración de Kaspersky Security Center actual como uno de reserva y luego utilícelo en el nuevo Servidor como certificado principal.

8 Configurar la conexión entre Kaspersky Thin Client y el nuevo Servidor de Kaspersky Security Center

Si existe un servidor DHCP en la infraestructura de su empresa y los ajustes para conectar Kaspersky Thin Client a Kaspersky Security Center se obtienen automáticamente, use la opción 224 para definir la dirección IP o el nombre de dominio del nuevo Servidor de administración de Kaspersky Security Center y espere a que todos los dispositivos con Kaspersky Thin Client completen su sincronización con Kaspersky Security Center.

Si no hay un servidor DHCP en la infraestructura de su empresa, [configure manualmente la conexión al nuevo servidor de Kaspersky Security Center en la interfaz de Kaspersky Thin Client](#).

Los grupos de administración de clientes ligeros quedan conectados al nuevo Kaspersky Security Center Server y puede administrarlos mediante la interfaz de Web Console.

Configurar los ajustes generales

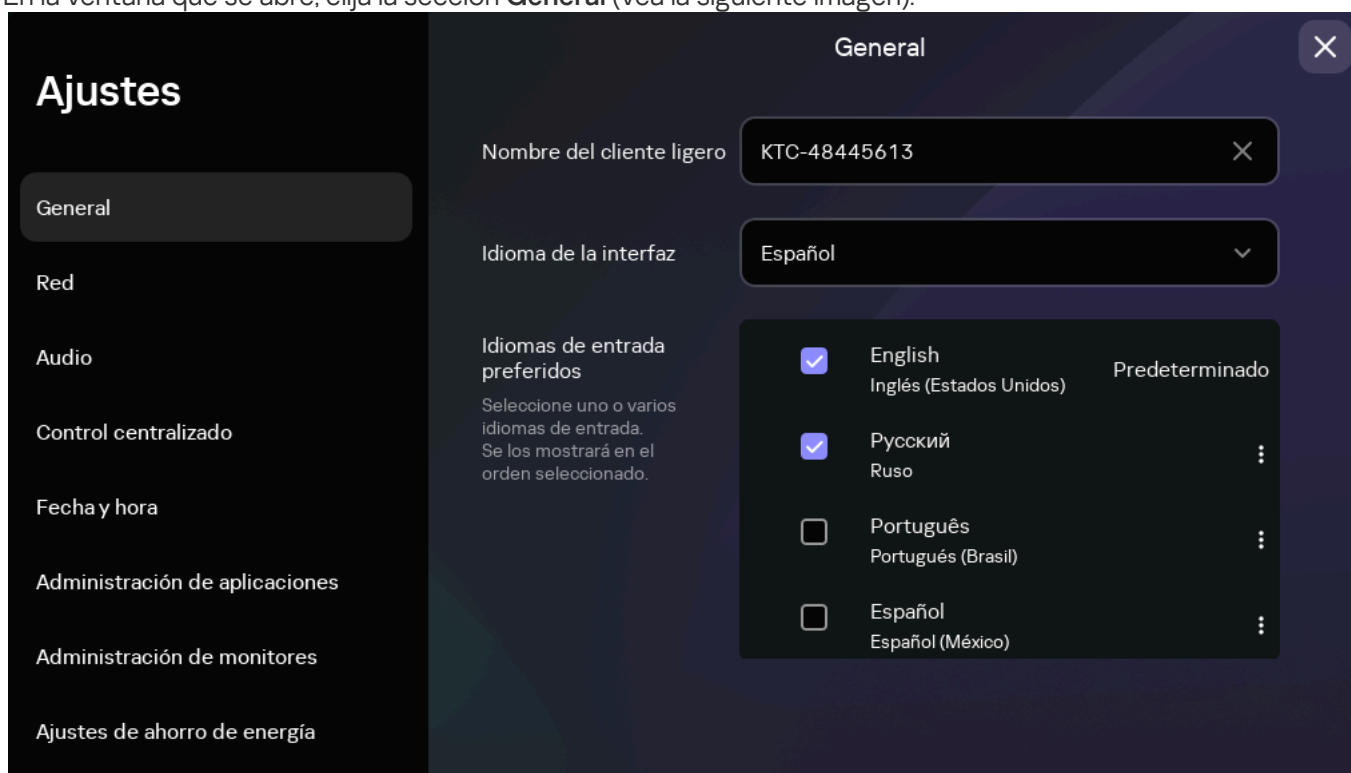
A través de la interfaz de Kaspersky Thin Client, puede configurar los ajustes generales del cliente ligero. Por ejemplo, puede definir el nombre que se muestra para el cliente ligero en la barra de tareas de Kaspersky Thin Client y en Kaspersky Security Center Web Console. También puede seleccionar el idioma que se usa para la interfaz de Kaspersky Thin Client.

Cuando un cliente ligero forma parte de un [grupo de administración](#), los valores de los ajustes que se detallan en este artículo se pueden imponer a través de Web Console. De ser este el caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

Es probable que los ajustes que se detallan en este artículo [no sean visibles en Kaspersky Thin Client](#).

Para configurar los ajustes generales de Kaspersky Thin Client:

1. En el panel de control de Kaspersky Thin Client, haga clic en , y, en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **General** (vea la siguiente imagen).



Ajustes. Sección General.

3. En el campo **Nombre del cliente ligero**, ingrese el nombre que se mostrará para Kaspersky Thin Client en Web Console. El nombre puede incluir letras mayúsculas y minúsculas de los alfabetos latino y cirílico, números y un guion. La longitud del nombre del cliente ligero no puede superar los treinta caracteres.
4. En la lista **Idioma de la interfaz**, seleccione el idioma de la interfaz de usuario. La interfaz de Kaspersky Thin Client 2.3 está disponible en los siguientes idiomas: ruso, inglés (EE. UU.), español (México) y portugués (Brasil).
5. En la lista desplegable **Idiomas de entrada preferidos**, seleccione uno o más idiomas. Kaspersky Thin Client admite los siguientes idiomas de entrada: inglés (EE. UU.), Ruso, español (México), alemán (estándar y Suiza), portugués (Brasil) y francés (Suiza). Los idiomas seleccionados se muestran en el panel de control de Kaspersky Thin Client en el orden que seleccionó y están disponibles al cambiar el idioma de entrada del teclado.

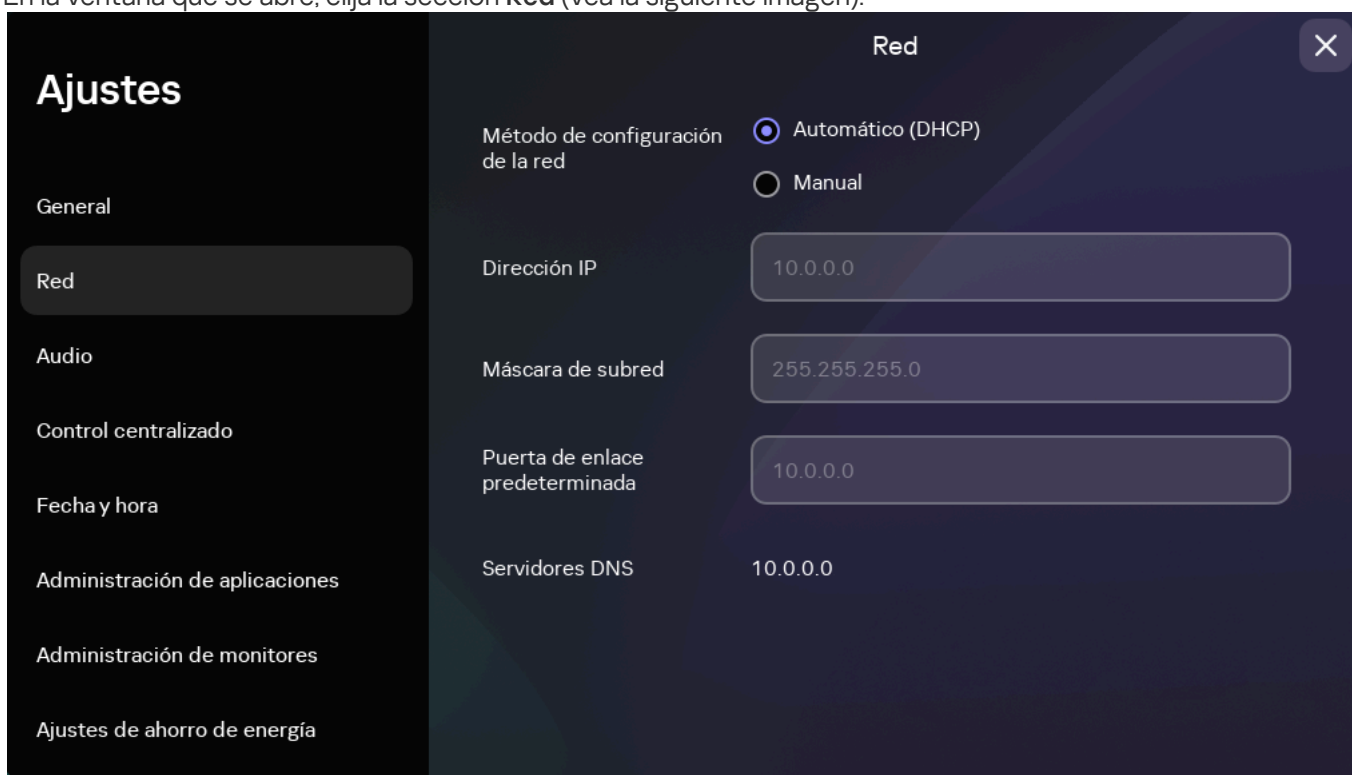
Los cambios se aplicarán una vez que reinicie el [cliente ligero](#).

Configurar los ajustes de la red

En la interfaz de Kaspersky Thin Client, puede configurar los ajustes para conectar Kaspersky Thin Client a la red.

Para configurar los ajustes de la red:

1. En el panel de control de Kaspersky Thin Client, haga clic en , y, en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Red** (vea la siguiente imagen).



Ajustes. Sección Red

3. Configure los ajustes para conectar Kaspersky Thin Client a la red:
 - Si desea obtener los ajustes de red automáticamente a través de DHCP, seleccione el valor **Automático (DHCP)** para el parámetro **Método de configuración de la red**. Si elige este valor, no podrá acceder a los campos **Dirección IP**, **Máscara de subred**, **Puerta de enlace predeterminada** y **Servidores DNS**.
 - Si desea definir los ajustes de red manualmente, seleccione el valor **Manual** para el parámetro **Método de configuración de la red** y haga lo siguiente:
 - En el campo **Dirección IP**, ingrese la dirección IP de Kaspersky Thin Client en formato IPv4.
 - En el campo **Máscara de subred**, ingrese la máscara de subred.
 - En el campo **Puerta de enlace predeterminada**, ingrese la dirección de la puerta de enlace de red.
 - En el campo **Servidores DNS**, ingrese las direcciones de los servidores DNS. Puede ingresar hasta dos direcciones.
4. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.

Administrar los dispositivos de reproducción y grabación de audio

Puede utilizar un conector para miniclavija o un puerto USB para conectar varios dispositivos de grabación y reproducción de audio a un cliente ligero con Kaspersky Thin Client para redirigirlos al entorno remoto. [Puede cambiar entre los dispositivos conectados](#) mediante la interfaz de Kaspersky Thin Client.

El volumen del audio y otros ajustes se controlan desde el entorno remoto.

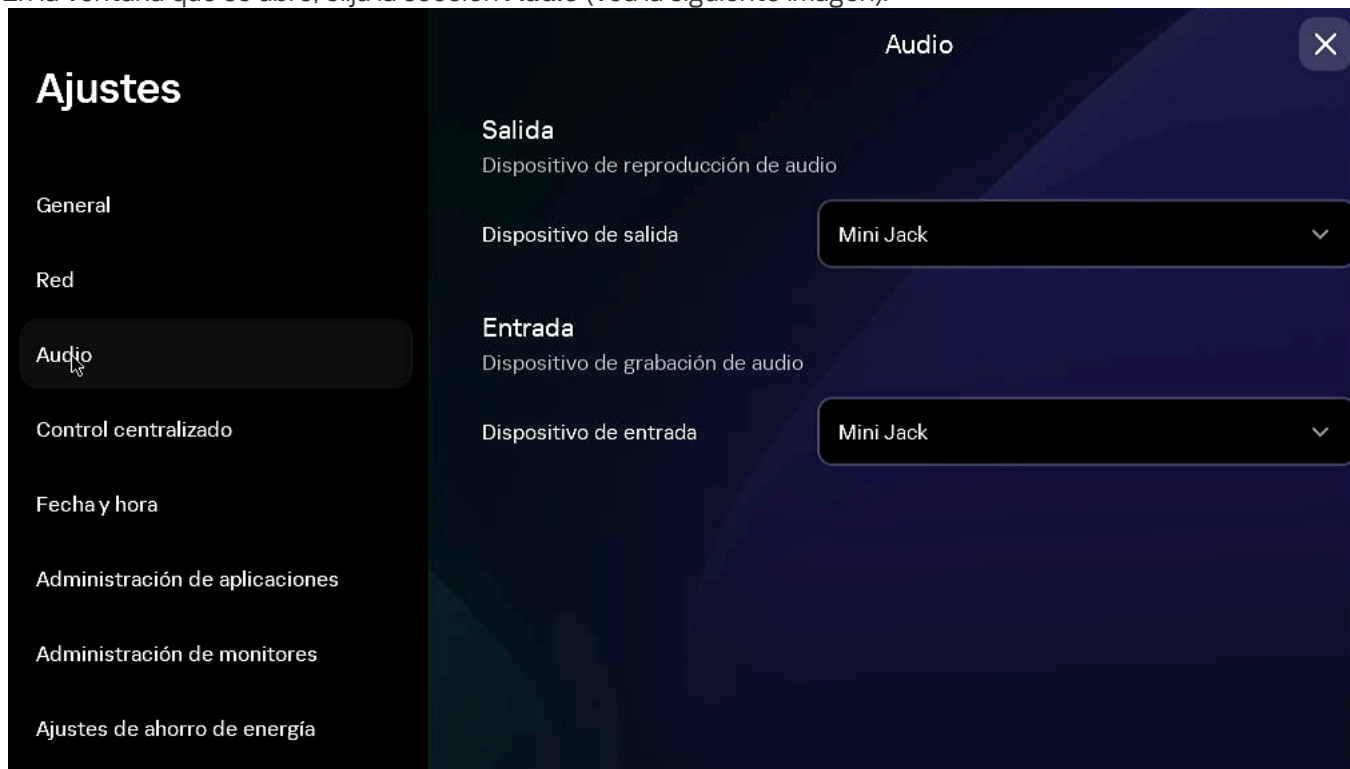
La conexión a través de un miniconector no es compatible con los clientes ligeros Dell Wyse 3040.

Cuando un cliente ligero forma parte de un [grupo de administración](#), los valores de los ajustes que se detallan en este artículo se pueden imponer a través de Web Console. De ser este el caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

Es probable que los ajustes que se detallan en este artículo [no sean visibles en Kaspersky Thin Client](#).

Para seleccionar los dispositivos de reproducción y grabación de audio que desee usar en Kaspersky Thin Client:

1. En el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Audio** (vea la siguiente imagen).



Ajustes. Sección de Audio

3. En la lista desplegable **Dispositivo de salida**, seleccione el dispositivo de reproducción de audio.
4. En la lista desplegable **Dispositivo de entrada**, seleccione el dispositivo de grabación de audio.

También puede utilizar dispositivos de reproducción y grabación de audio en un entorno remoto y [alternar entre ellos desde el panel de conexión](#).

Configurar los ajustes para conectar Kaspersky Thin Client a Kaspersky Security Center

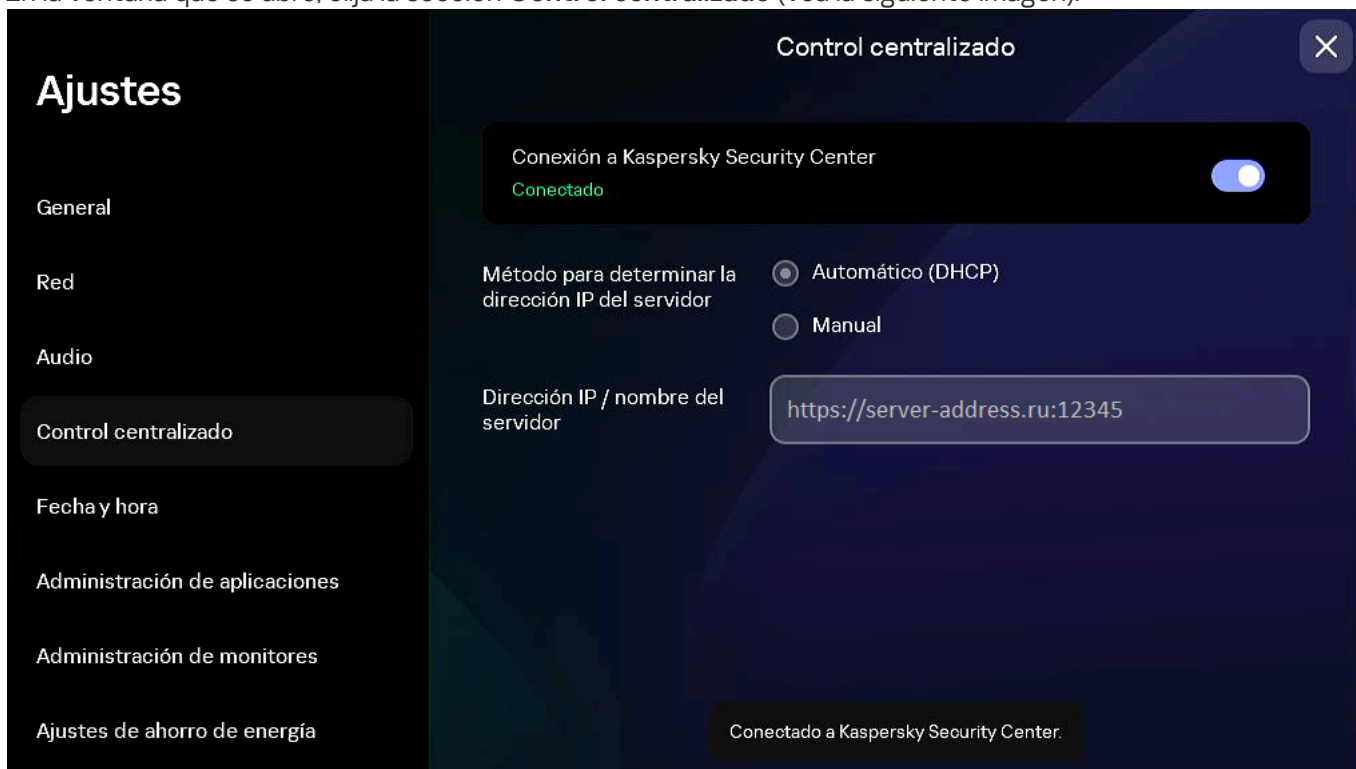
Para administrar un cliente ligero a través de Web Console, debe configurar los ajustes para conectar Kaspersky Thin Client al Servidor de administración de Kaspersky Security Center (en adelante, también denominado simplemente "Kaspersky Security Center").

Le recomendamos recurrir a los servicios de un especialista cualificado de su empresa para configurar la conexión de Kaspersky Thin Client con Kaspersky Security Center y verificar la autenticidad del certificado aceptado.

Para asegurarse de obtener las actualizaciones de seguridad importantes de los servidores de actualización de Kaspersky, recomendamos que utilice un Servidor de administración de Kaspersky Security Center independiente para administrar los clientes ligeros. Esto se debe a que cada Servidor de administración de Kaspersky Security Center puede tener una única [tarea de actualización](#) activa, con un único origen de actualización prioritario.

Para configurar los ajustes que permiten conectar Kaspersky Thin Client al Servidor de administración de Kaspersky Security Center:

1. En el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Control centralizado** (vea la siguiente imagen).



Ajustes. Sección Control centralizado

3. En la ventana **Control centralizado**, configure los siguientes ajustes para conectar Kaspersky Thin Client a Kaspersky Security Center:

- Si desea que los ajustes para conectar Kaspersky Thin Client a Kaspersky Security Center se obtengan automáticamente a través del protocolo DHCP, seleccione **Automático (DHCP)** en el bloque **Método para determinar la dirección IP del servidor**. Si elige este modo, no podrá hacer cambios en el campo **Dirección IP / nombre del servidor**.

Para usar esta opción de conexión, debe existir un servidor DHCP en la infraestructura de la empresa y debe usarse la opción 224 para definir la dirección IP o el nombre de dominio del Servidor de administración de Kaspersky Security Center al que deba conectarse Kaspersky Thin Client. El sistema Kaspersky Thin Client recibe valores de cadena en formato **dirección IP:puerto** o **nombre del Servidor:puerto** en la opción 224. Por ejemplo, 192.168.2.4 o ksc.example.com:12345. El puerto debe indicarse solo si la conexión se realiza a través de un puerto que no sea el 13292.

De manera predeterminada, el uso de DHCP está habilitado a fin de obtener automáticamente los ajustes para conectar Kaspersky Thin Client a Kaspersky Security Center.

- Si desea definir manualmente los ajustes para conectar Kaspersky Thin Client a Kaspersky Security Center, seleccione **Manual** en el bloque **Método para determinar la dirección IP del servidor** y, en el campo **Dirección IP / nombre del servidor**, ingrese la dirección IP o el nombre del Servidor de administración de Kaspersky Security Center. Si utiliza un puerto que no sea el 13292, indíquelo siguiendo el formato **dirección IP:puerto** o **nombre del Servidor:puerto**.

4. Active el interruptor **Conexión a Kaspersky Security Center**.

5. Cuando se conecte a Kaspersky Security Center por primera vez, en la ventana **Agregar certificado**, revise los parámetros del certificado utilizado para conectar Kaspersky Thin Client a Kaspersky Security Center. A continuación, haga clic en el botón **Agregar certificado**. El certificado agregado se utilizará de allí en adelante para las conexiones entre Kaspersky Thin Client y Kaspersky Security Center.

Si el certificado utilizado para conectar Kaspersky Thin Client a Kaspersky Security Center se modifica en Kaspersky Security Center, deberá [confirmar el cambio de certificado](#) para poder configurar la conexión.

Kaspersky Thin Client intentará conectarse a Kaspersky Security Center. Cuando se establezca la conexión con Kaspersky Security Center, se mostrará el estado **Conectado a Kaspersky Security Center**.

Modificar los ajustes de conexión a Kaspersky Thin Client a Kaspersky Security Center

Cuando un cliente ligero forma parte de un [grupo de administración](#), los valores de los ajustes que se detallan en este artículo se pueden imponer a través de Web Console. De ser este el caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

Es probable que los ajustes que se detallan en este artículo [no sean visibles en Kaspersky Thin Client](#).

Para cambiar los ajustes que se utilizan para conectar Kaspersky Thin Client a Kaspersky Security Center:

1. En el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Control centralizado**.

3. Desactive el interruptor **Conexión a Kaspersky Security Center**.
4. Se abre una ventana llamada **Confirmar desconexión**. Memorice el código de confirmación que aparece en la ventana y envíeselo al administrador de Kaspersky Security Center. Encontrará los datos de contacto del administrador en la ventana **Confirmar desconexión**. El administrador le enviará un código de confirmación como respuesta.
5. Haga clic en **Siguiente**.
6. Se abre una ventana llamada **Código de confirmación**. Ingrese el código que le haya brindado el administrador de Kaspersky Security Center y haga clic en el botón **Confirmar**.
Kaspersky Thin Client dejará de estar administrado por Kaspersky Security Center.
7. En la ventana **Control centralizado**, [configure manualmente los ajustes de conexión a Kaspersky Security Center](#).
8. Active el interruptor **Conexión a Kaspersky Security Center**.
El cliente ligero intentará conectarse a Kaspersky Security Center. Cuando se establezca la conexión con Kaspersky Security Center, se mostrará el estado **Conectado a Kaspersky Security Center**.

Configurar la fecha y la hora

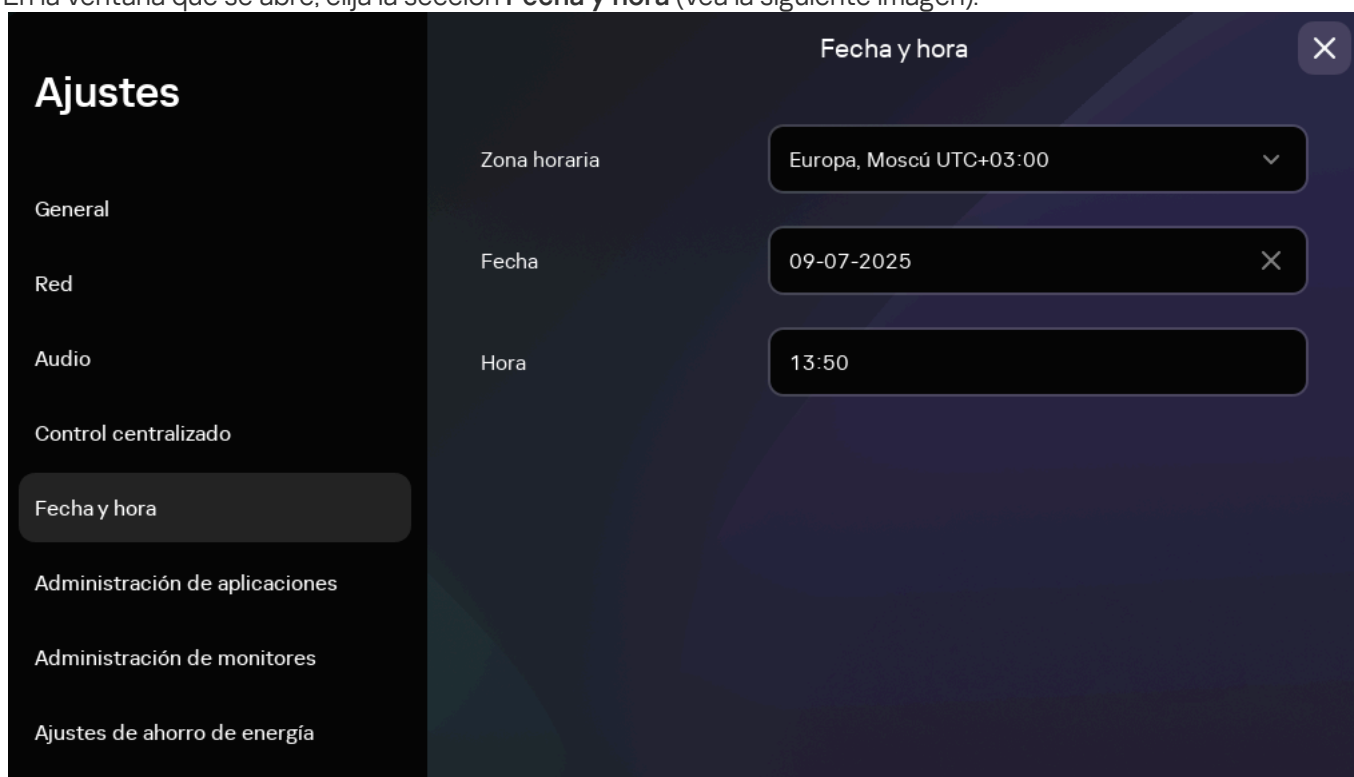
Los clientes ligeros conectados a Kaspersky Security Center obtienen la fecha y la hora del Servidor de administración de Kaspersky Security Center. Puede cambiar manualmente la fecha y la hora en Kaspersky Thin Client únicamente si el sistema no se controla a través de Kaspersky Security Center.

Cuando un cliente ligero forma parte de un [grupo de administración](#), los valores de los ajustes que se detallan en este artículo se pueden imponer a través de Web Console. De ser este el caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

Es probable que los ajustes que se detallan en este artículo [no sean visibles en Kaspersky Thin Client](#).

Para cambiar la fecha y la hora en Kaspersky Thin Client:

1. En el panel de control de Kaspersky Thin Client, haga clic en , en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Fecha y hora** (vea la siguiente imagen).



Ajustes. Sección Fecha y hora.

3. Configure los ajustes de fecha y hora:

- Seleccione la zona horaria que corresponda en la lista desplegable **Zona horaria**.
- En el campo **Fecha**, ingrese la fecha presente en formato DD-MM-AAAA.
- En el campo **Hora**, ingrese la hora presente en formato HH:MM:SS.

4. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.

Configurar el inicio automático y la visualización de aplicaciones

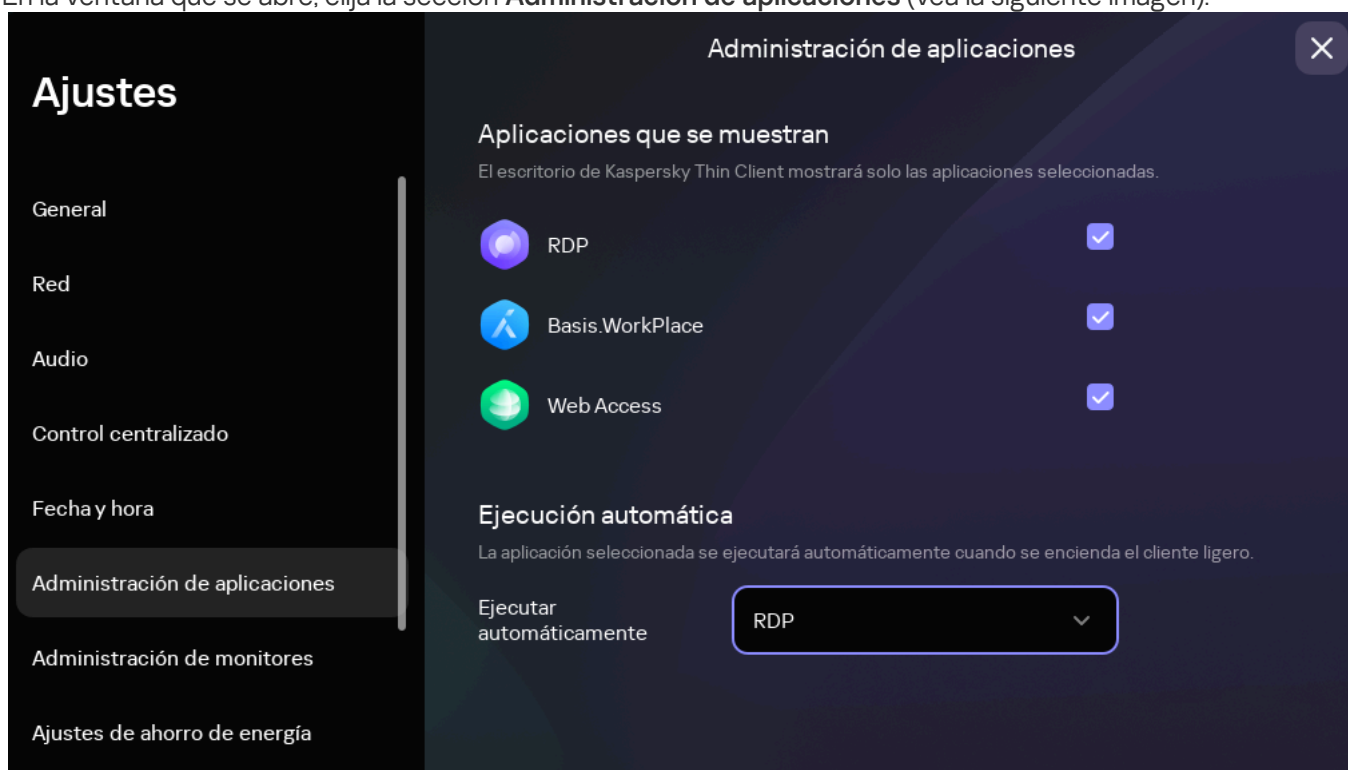
Puede seleccionar una [aplicación](#) que se ejecutará automáticamente después de iniciar el dispositivo y el sistema, y puede especificar qué aplicaciones se mostrarán en el escritorio de Kaspersky Thin Client.

Cuando un cliente ligero forma parte de un [grupo de administración](#), los valores de los ajustes que se detallan en este artículo se pueden imponer a través de Web Console. De ser este el caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

Es probable que los ajustes que se detallan en este artículo [no sean visibles en Kaspersky Thin Client](#).

Para configurar el inicio automático y la visualización de aplicaciones:

1. En el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Administración de aplicaciones** (vea la siguiente imagen).



Ajustes. Sección Administración de aplicaciones

3. En el bloque **Aplicaciones que se muestran**, seleccione las casillas de verificación junto a las aplicaciones que se mostrarán en el escritorio de Kaspersky Thin Client.
4. En la lista desplegable **Ejecutar automáticamente**, seleccione la aplicación que se ejecutará automáticamente después de encender el dispositivo y arrancar el sistema. Si selecciona **Deshabilitado**, el inicio automático se desactivará.

Los cambios se guardarán y aplicarán.

También puede [configurar la conexión automática a un entorno remoto en la aplicación RDP](#) para iniciar una sesión remota después de iniciar Kaspersky Thin Client.

Configurar los monitores y pantallas

Kaspersky Thin Client permite conectar dos monitores.

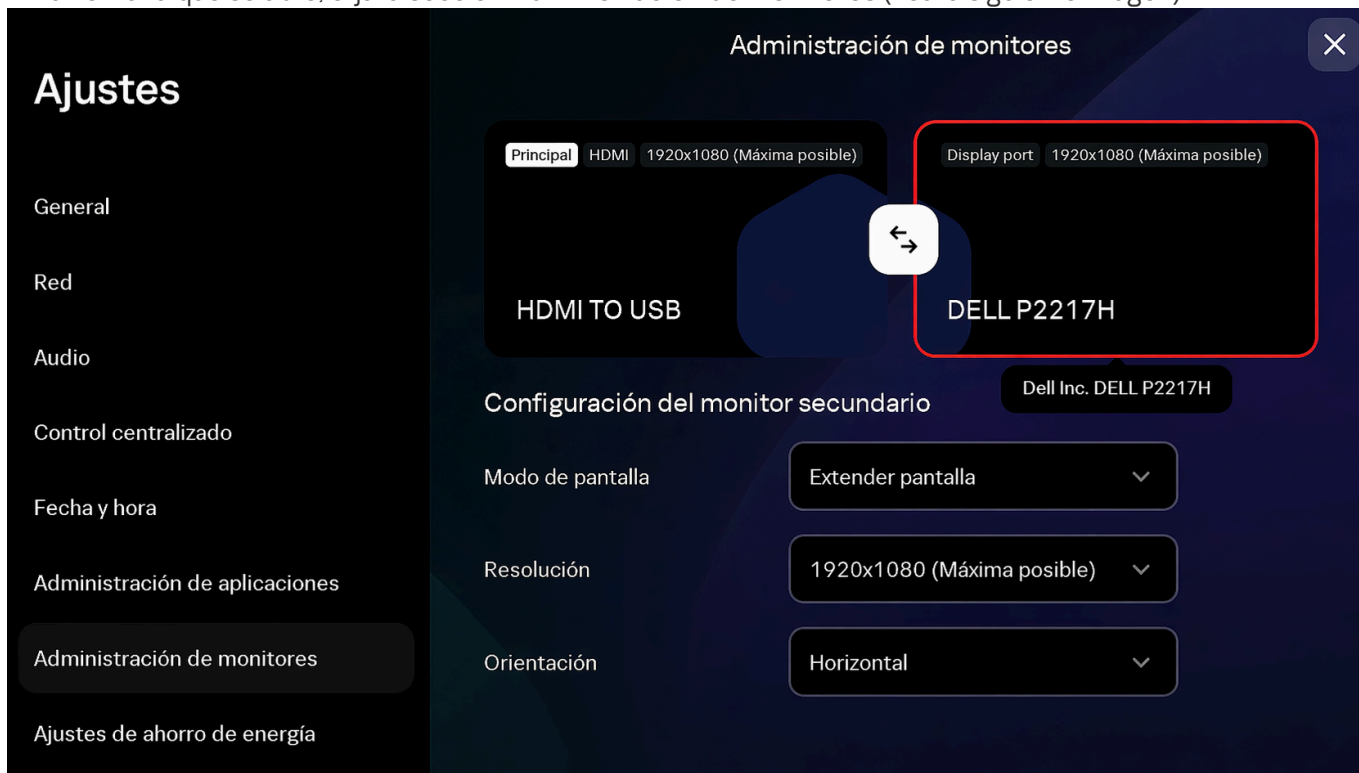
Cuando se conectan dos monitores, el sistema considera que uno es el principal y el otro el secundario. Durante una [sesión remota](#), el panel de conexión se muestra en la pantalla del monitor principal. La pantalla del monitor secundario amplía o duplica la imagen del monitor principal. En la interfaz de Kaspersky Thin Client, puede seleccionar qué monitor debe considerarse principal (en adelante también "cambiar el diseño del monitor").

Si desea que la pantalla de la sesión remota se muestre en ambos monitores, habilítelos en la configuración de conexión del entorno de conexión remota en las aplicaciones [RDP](#) o [Basis.WorkPlace](#).

Mediante la interfaz de Kaspersky Thin Client, puede ver información sobre los monitores conectados al cliente ligero y cambiar la disposición de las pantallas. También puede configurar los ajustes de pantalla que se aplican a cada monitor.

Para configurar monitores y pantallas:

1. En el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Administración de monitores** (vea la siguiente imagen).



Ajustes. Sección Administración de monitores

3. Si tiene dos monitores conectados a su cliente ligero, puede cambiar su diseño. Para ello, haga clic en el botón .

4. Si desea personalizar la pantalla de un monitor específico, seleccione el monitor. Para ello, haga clic en su imagen esquemática.

Para resaltar el monitor que vas a personalizar, pasa el cursor sobre la imagen esquemática de los monitores. Aparece un marco rojo en la imagen del monitor personalizado.

5. Configure los ajustes necesarios:

- En la lista desplegable **Modo de pantalla**, seleccione la opción de visualización de imagen:
 - **Extender pantalla:** la imagen se extiende a lo largo de dos monitores.
 - **Duplicar pantalla:** la imagen de la pantalla del monitor principal se duplica en el secundario. Si esta opción está seleccionada, los siguientes ajustes no estarán disponibles para la pantalla adicional.

Esta opción solo se muestra si hay dos monitores conectados al cliente ligero.

- En la lista desplegable **Resolución**, seleccione la resolución que desea para la pantalla seleccionada. Las resoluciones admitidas se enumeran [en la sección de requisitos de hardware y software](#).

Si el valor **Máxima posible** está seleccionado, se establece el valor más alto del parámetro admitido por el monitor y por Kaspersky Thin Client.

- En la lista desplegable **Orientación**, seleccione la posición de la pantalla:
 - **Horizontal**: la posición estándar de la pantalla.
 - **Horizontal invertido**: la pantalla gira 180°.
 - **Vertical**: la pantalla gira 90°.
 - **Vertical invertido**: la pantalla gira 270°.

Cuando cambie un valor de configuración por otro, aparecerá una ventana con una cuenta regresiva.

6. En esta ventana, haga clic en **Guardar** para confirmar los cambios. Si desea descartar los cambios realizados y seguir personalizando la configuración, haga clic en **Cancelar**.

Los cambios se guardarán.

Configurar los ajustes de ahorro de energía

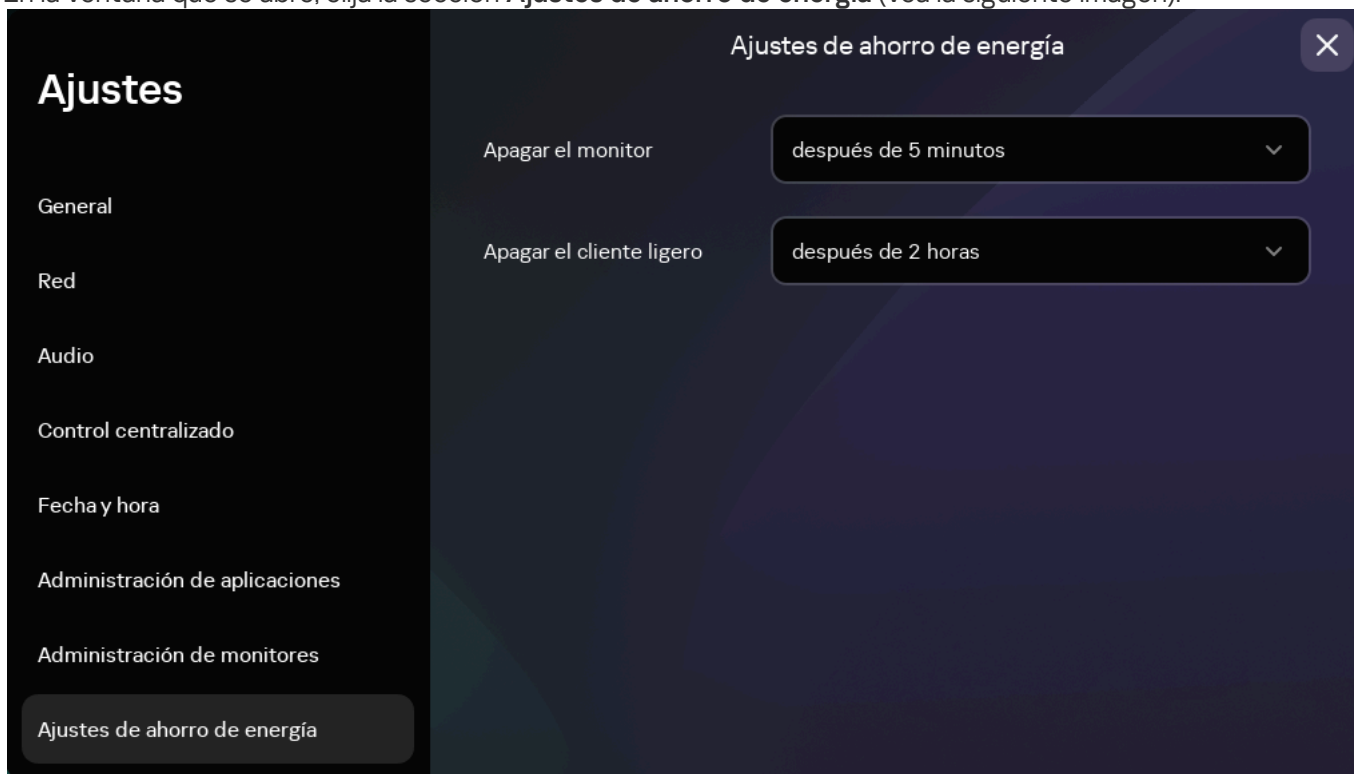
Cuando un cliente ligero forma parte de un [grupo de administración](#), los valores de los ajustes que se detallan en este artículo se pueden imponer a través de Web Console. De ser este el caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

Es probable que los ajustes que se detallan en este artículo [no sean visibles en Kaspersky Thin Client](#).

Puede configurar un período de inactividad tras el cual se apague el monitor. El monitor se encenderá automáticamente cuando se haga clic con el mouse, se mueva el puntero o se presione una tecla en el teclado. También puede definir si, transcurrido un tiempo específico sin actividad, el cliente ligero con Kaspersky Thin Client deberá apagarse. Para seguir utilizando el cliente ligero, será necesario encenderlo de nuevo.

Para configurar los ajustes de ahorro de energía:

1. En el panel de control de Kaspersky Thin Client, haga clic en , en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Ajustes de ahorro de energía** (vea la siguiente imagen).



Ajustes. Sección Ajustes de ahorro de energía

3. En la lista desplegable **Apagar el monitor**, seleccione el período de inactividad del sistema después del cual se apagará el monitor.
4. En la lista desplegable **Apagar el cliente ligero**, seleccione el período de inactividad del sistema después del cual el cliente ligero se apagará.

También puede configurar los ajustes de ahorro de energía mediante la interfaz de Kaspersky Security Center Web Console.

Configurar los ajustes para la administración remota de clientes ligeros en la interfaz de Kaspersky Thin Client

Cuando un cliente ligero forma parte de un [grupo de administración](#), los valores de los ajustes que se detallan en este artículo se pueden imponer a través de Web Console. De ser este el caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

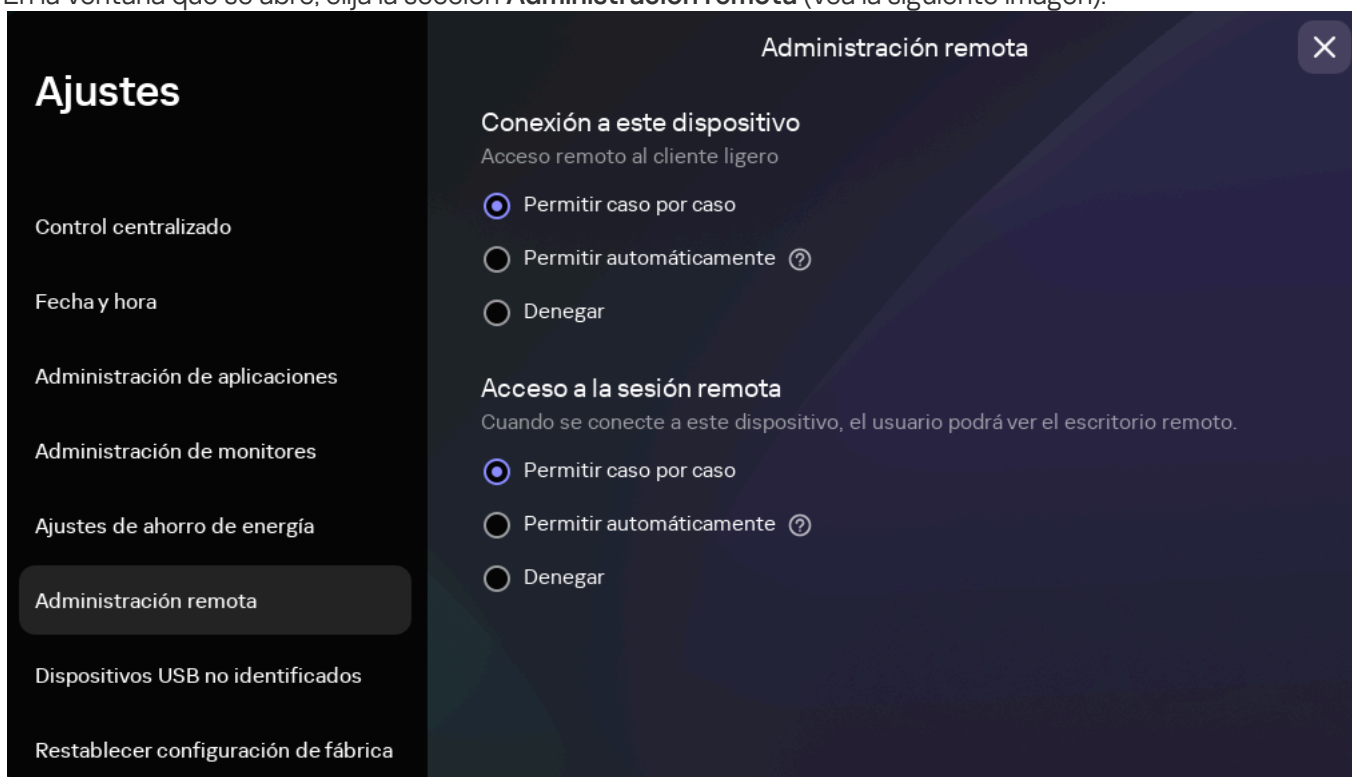
Es probable que los ajustes que se detallan en este artículo [no sean visibles en Kaspersky Thin Client](#).

En la interfaz de Kaspersky Thin Client, puede configurar los siguientes ajustes de [administración remota](#):

- **Modo de acceso a la capacidad de administración remota.**
Determina las condiciones y el procedimiento para conectarse al cliente ligero.
- **Modo de acceso a la sesión remota que esté activa en el cliente ligero al establecer conexión con él** (en lo sucesivo, para referirse a esta sesión, también se usará el término "pantalla del entorno remoto").
Puede restringir el acceso a la pantalla del entorno remoto si el usuario del cliente ligero trabaja con datos confidenciales o privados.

Para configurar los ajustes para la administración remota de un cliente ligero:

1. [Encienda el cliente ligero.](#)
2. En el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Ajustes**.
3. En la ventana que se abre, elija la sección **Administración remota** (vea la siguiente imagen).



Ajustes. Sección Administración remota

4. En el grupo de opciones **Conexión a este dispositivo**, seleccione el modo de acceso a la capacidad de administración remota del cliente ligero:

- **Permitir automáticamente**

Si selecciona este modo, el administrador podrá conectarse al cliente ligero remoto después de que el usuario [acepte la solicitud de administración remota en la interfaz de Kaspersky Thin Client](#). Si el usuario rechaza la solicitud, la conexión se finalizará. Si no hay respuesta en 30 segundos, la conexión se establece automáticamente.

Para garantizar la seguridad del dispositivo, sugerimos usar este modo solo si el cliente ligero está conectado a Kaspersky Security Center.

- **Permitir caso por caso**

En este modo, el administrador podrá conectarse de forma remota al cliente ligero solo después de que el usuario [acepte la solicitud de administración remota en la interfaz de Kaspersky Thin Client](#). Si el usuario rechaza la solicitud, la conexión se finalizará.

- **Denegar**

Si selecciona este modo, el administrador no podrá conectarse al cliente ligero remoto.

Si selecciona los modos **Permitir automáticamente** o **Permitir caso por caso**, se mostrará el grupo de opciones **Acceso a la sesión remota**.

5. En el grupo de opciones **Acceso a la sesión remota**, seleccione el modo de acceso a la pantalla del entorno remoto:

- **Permitir automáticamente**

Si selecciona este modo, tras conectarse al cliente ligero, el administrador podrá acceder a la pantalla del entorno remoto sin que el usuario confirme la acción.

- **Permitir caso por caso**

Si selecciona este modo, tras conectarse al cliente ligero, el administrador podrá acceder a la pantalla del entorno remoto únicamente si el usuario [confirma la solicitud de acceso en la interfaz de Kaspersky Thin Client](#).

- **Denegar**

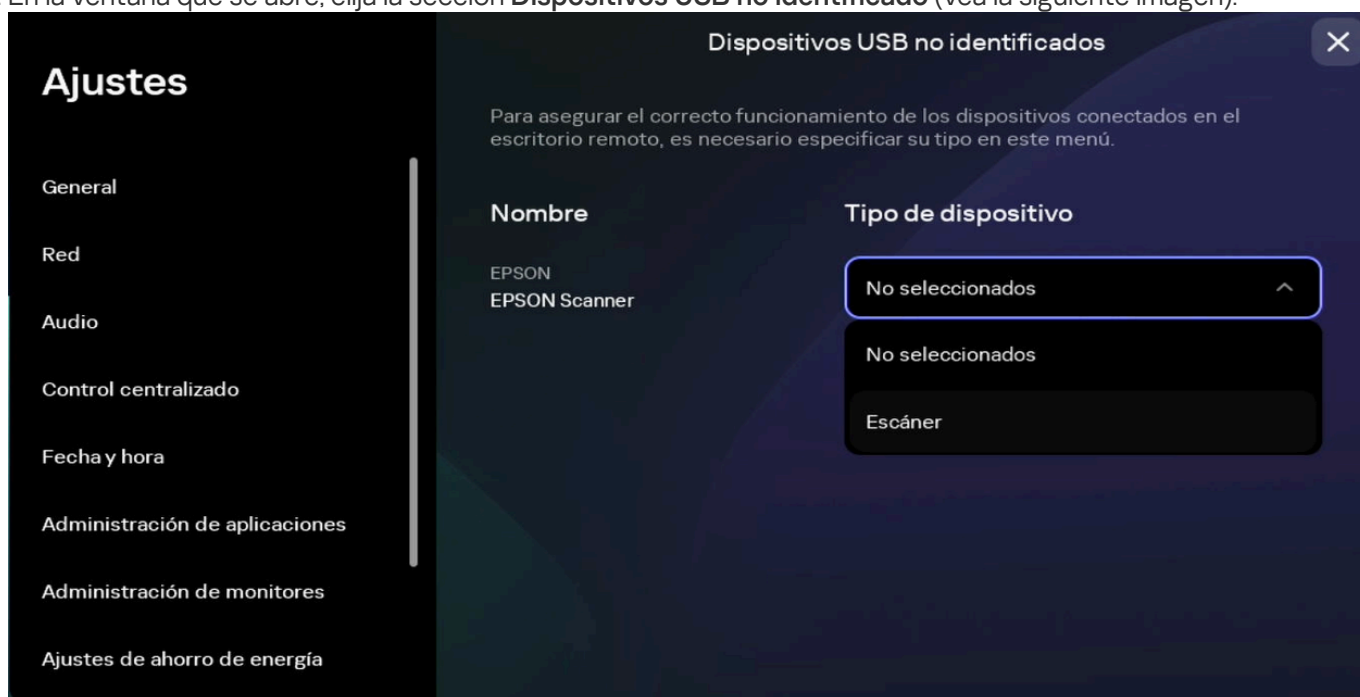
Si selecciona este modo, el administrador no podrá administrar el cliente ligero a distancia hasta que el usuario [cierre manualmente su sesión remota](#).

Cambiar el tipo de dispositivos USB no identificados

De forma predeterminada, Kaspersky Thin Client detecta automáticamente el tipo de [dispositivo USB compatible](#) conectado al cliente ligero. Si el sistema no puede determinar el tipo de dispositivo conectado (en lo sucesivo, también denominado "dispositivo no identificado"), debe seleccionar manualmente el tipo en la interfaz de Kaspersky Thin Client para garantizar su correcto funcionamiento.

Para cambiar manualmente el tipo de un dispositivo USB no identificado:

1. En el panel de control de Kaspersky Thin Client, haga clic en , y, en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Dispositivos USB no identificado** (vea la siguiente imagen).



Ajustes. Sección Dispositivos USB no identificados

Verá una lista de dispositivos USB cuyo tipo no pudo identificar el sistema. Se muestra el nombre del modelo y el fabricante de cada dispositivo si el sistema logra obtener esta información.

Si no se detectaron dispositivos no identificados, la lista estará vacía.

3. En la lista desplegable junto al nombre del dispositivo correspondiente, seleccione su tipo.

En la versión actual de Kaspersky Thin Client, solo está disponible el siguiente tipo de dispositivo USB: escáner.

El tipo de dispositivo no reconocido se cambiará y se guardará en el sistema. Ahora puede [redireccionar el dispositivo a un entorno remoto](#).

Restablecer la configuración de Kaspersky Thin Client

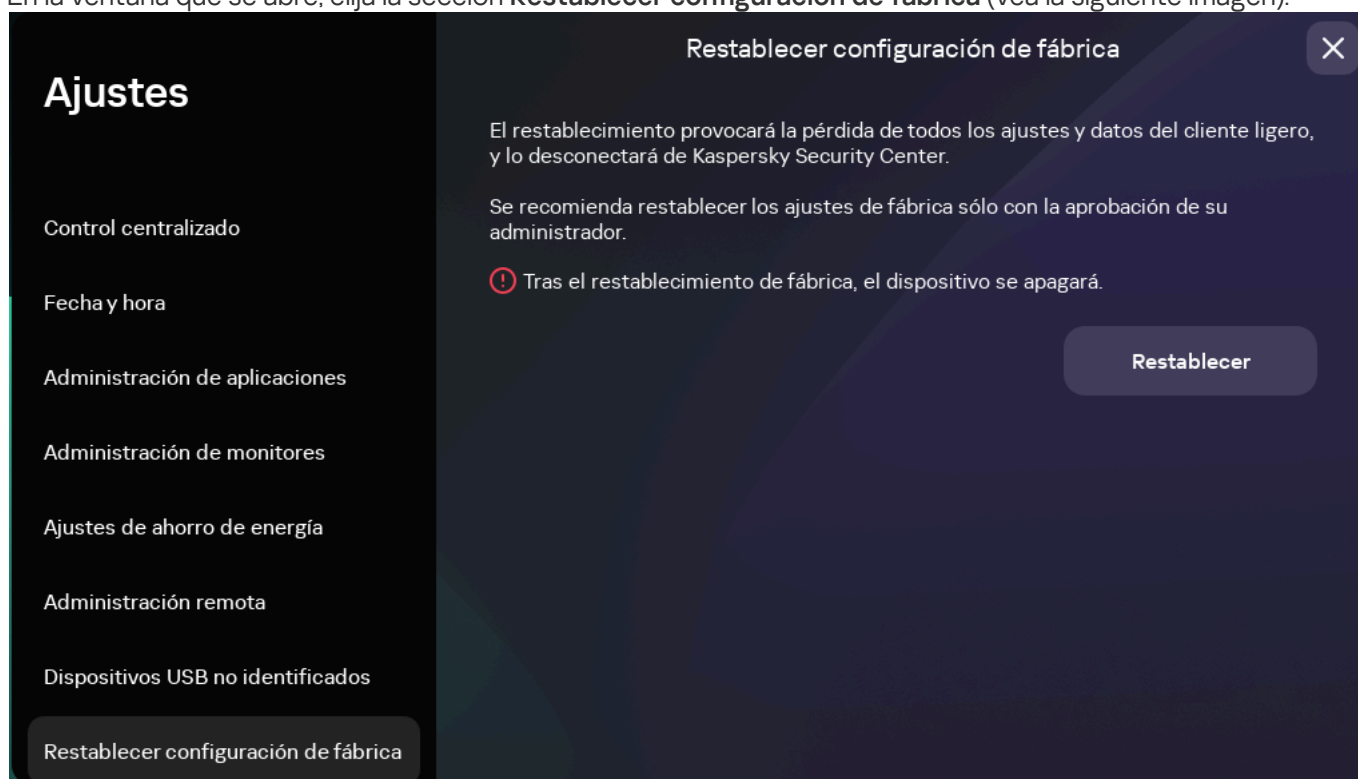
Cuando se lleva a cabo un restablecimiento, se eliminan todos los ajustes definidos y todos los datos de Kaspersky Thin Client (excepto el [registro de auditoría](#) y la fecha del sistema). También se desconecta el dispositivo de Kaspersky Security Center. Recomendamos llevar a cabo un restablecimiento solo si lo ha aprobado el administrador de la empresa.

Cuando un cliente ligero forma parte de un [grupo de administración](#), los valores de los ajustes que se detallan en este artículo se pueden imponer a través de Web Console. De ser este el caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

Es probable que los ajustes que se detallan en este artículo [no sean visibles en Kaspersky Thin Client](#).

Para restablecer la configuración de Kaspersky Thin Client:

1. En el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Restablecer configuración de fábrica** (vea la siguiente imagen).



Ajustes. Sección Restablecer configuración de fábrica

Como resultado, se restablecerán los valores originales (predeterminados) de todos los ajustes de Kaspersky Thin Client, se eliminarán todos los datos del dispositivo (excepto el [registro de auditoría](#) y la fecha del sistema) y Kaspersky Thin Client se desconectará de Kaspersky Security Center. Cuando se complete el restablecimiento, el cliente ligero se apagará.

Para restablecer la configuración de fábrica de un cliente ligero que forma parte de un grupo de administración:

1. En el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Ajustes**.
2. En la ventana que se abre, elija la sección **Restablecer configuración de fábrica**.

3. En la ventana que se abre, haga clic en el botón **Restablecer**.

Se abre la ventana **Confirmar reinicio**, en la cual se muestra un código de confirmación.

4. Bríndele el código de confirmación al administrador de Kaspersky Security Center. Encontrará los datos de contacto del administrador en la ventana **Confirmar reinicio**. El administrador de Kaspersky Security Center le responderá con un código de confirmación.

5. Haga clic en **Siguiente**.

6. Se abre una ventana llamada **Código de confirmación**. Ingrese el código que le haya brindado el administrador de Kaspersky Security Center y haga clic en el botón **Confirmar**.

Como resultado, se restablecerán los valores originales (predeterminados) de todos los ajustes de Kaspersky Thin Client, se eliminarán todos los datos del dispositivo (excepto el [registro de auditoría](#) y la fecha del sistema) y Kaspersky Thin Client se desconectará de Kaspersky Security Center. Cuando se complete el restablecimiento, el cliente ligero se apagará.

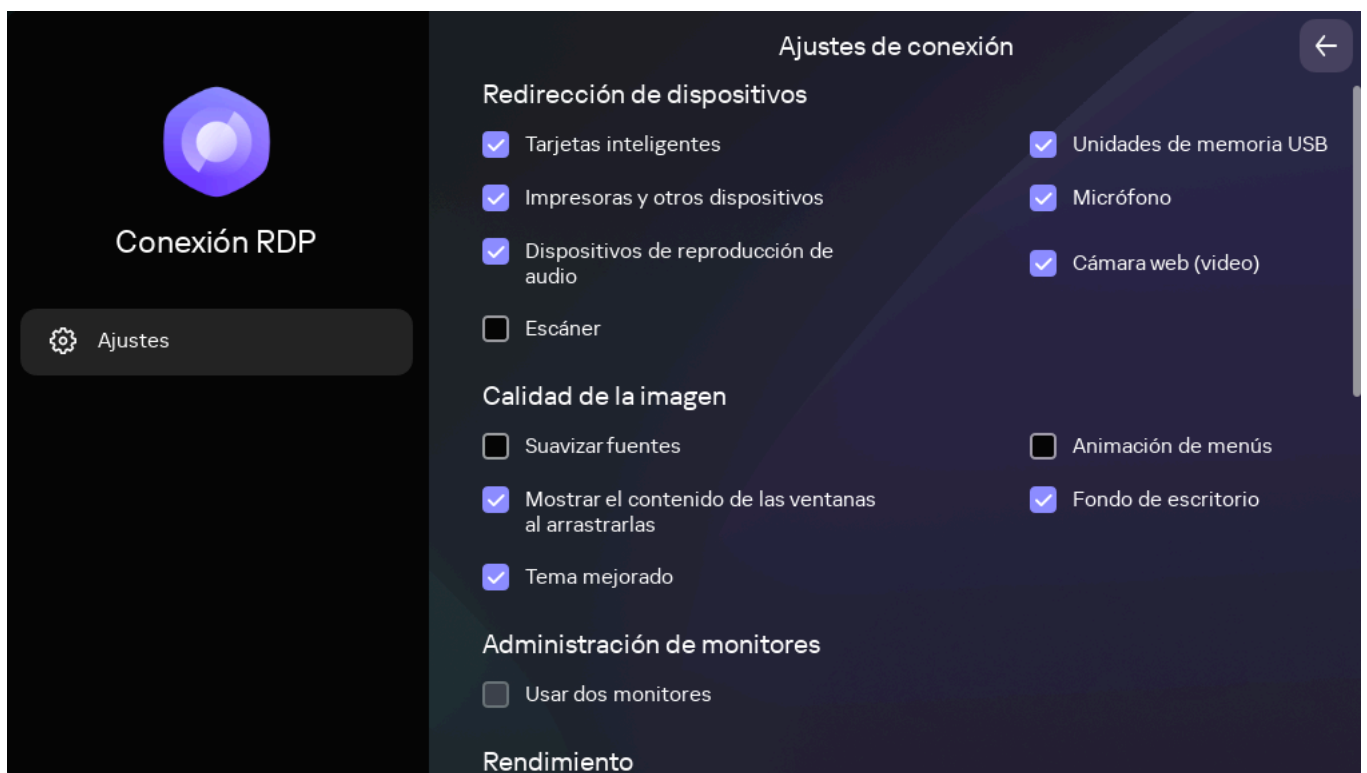
Configurar los ajustes para conectarse a un entorno remoto usando la aplicación RDP

En la aplicación RDP, puede configurar los ajustes de [conexión a una aplicación virtual o escritorio remoto](#) a través de RDP, incluyendo la conexión automática a un entorno remoto.

Para configurar los ajustes para conectarse a un entorno remoto en la aplicación RDP:

1. En el escritorio de Kaspersky Thin Client, haga clic en el botón **RDP**.
2. En la parte izquierda de la ventana de conexión que se abre, haga clic en **Ajustes**.

Se abre una ventana para configurar los ajustes que se usarán al conectarse al entorno remoto (vea la siguiente imagen).



Ventana para configurar una conexión a un entorno remoto en la aplicación RDP

3. En el bloque de ajustes **Redirección de dispositivos**, seleccione los dispositivos que se redirigirán al entorno remoto: **Tarjetas inteligentes**, **Unidades de memoria USB**, **Impresoras y otros dispositivos**, **Micrófono**, **Dispositivos de reproducción de audio**, **Cámara web (video)**, **Escáner**.

El volumen del audio y otros ajustes se controlan desde el entorno remoto.

Para redireccionar dispositivos USB a un escritorio remoto que ejecute el sistema operativo Windows 10, es necesario habilitar los Servicios de Escritorio remoto de Microsoft y permitir la redirección de dispositivos Plug and Play en la configuración de los Servicios de Escritorio remoto. En el caso de Microsoft Windows Server 2016 o 2019, también se deben permitir las conexiones remotas a través de los Servicios de Escritorio remoto y se debe permitir la configuración de reglas de control remoto en los Servicios de Escritorio remoto.

4. En el bloque **Calidad de la imagen**, seleccione las casillas junto a la configuración gráfica del escritorio remoto que desea usar: **Suavizar fuentes**, **Animación de menús**, **Fondo de escritorio**, **Mostrar el contenido de las ventanas al arrastrarlas**, **Tema mejorado**.

Si habilita las opciones gráficas del escritorio remoto, podría verse afectada la velocidad de las operaciones de Kaspersky Thin Client.

5. Si su estación de trabajo tiene dos monitores y desea que la imagen del escritorio remoto se muestre en ambos, marque la casilla **Usar dos monitores** en el bloque **Administración de monitores**.
6. Para mejorar el rendimiento cuando se conecte a aplicaciones o escritorios remotos, en el bloque **Rendimiento**, marque **Mejorar el rendimiento gráfico**.
7. Para [conectarse automáticamente a un escritorio remoto o una aplicación virtual](#) cuando se inicia la aplicación RDP, en el bloque **Conexión automática**, seleccione la casilla **Conexión automática**.

Para activar la función, debe conectarse manualmente y desconectarse del entorno remoto una vez. Cuando lo hace, los siguientes datos para conectarse al servidor RDP se guardan en el almacenamiento del cliente ligero: nombre de usuario, dirección del servidor y contraseña. La siguiente vez que inicie la aplicación RDP, estas credenciales se usarán para iniciar automáticamente una conexión con el entorno remoto. Si deshabilita la función de conexión automática, la contraseña guardada se elimina del almacenamiento del dispositivo.

Para establecer una conexión automática al entorno remoto en la aplicación RDP inmediatamente después de iniciar Kaspersky Thin Client, [configure el inicio automático de la aplicación](#) en la sección **Ajustes**.
8. Si desea usar el Agente de conexión a Escritorio remoto de Microsoft para conectarse a un escritorio remoto, en el campo **Id. de colección del Agente de conexión a Escritorio remoto**, ingrese el id. de la colección en formato `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` hace referencia al identificador específico de la colección).

Si desea iniciar una aplicación virtual, ingrese el alias de la aplicación en el campo **Alias de la aplicación**.
9. Si desea que la conexión se restablezca automáticamente ante una desconexión inesperada, marque la casilla **Conectar de nuevo si se pierde la conexión**.
10. Haga clic en la flecha hacia atrás en la esquina superior derecha de la ventana para regresar a la ventana de conexión.

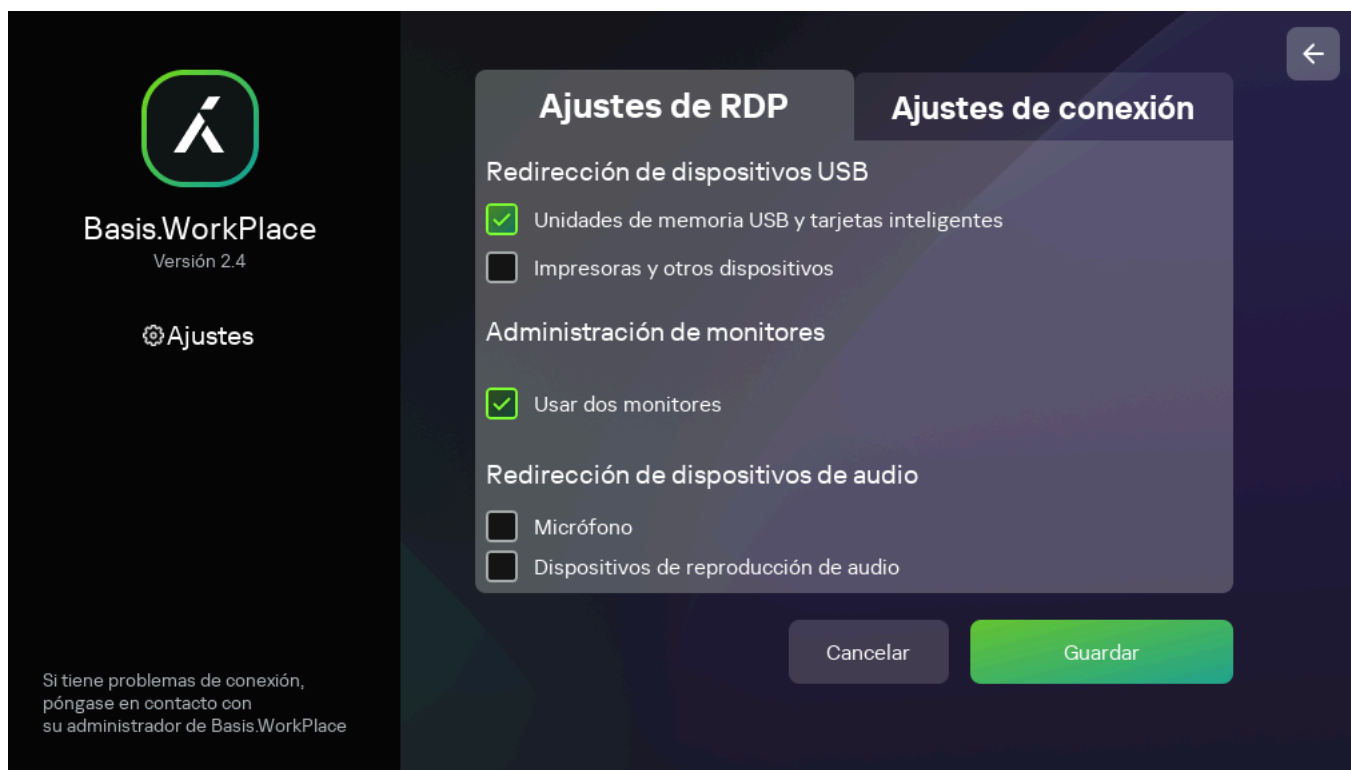
Configurar los ajustes para conectarse a un entorno remoto usando la aplicación de Basis.WorkPlace

Usando la aplicación Basis.WorkPlace, puede configurar los ajustes que se usarán para conectarse a un entorno remoto implementado en la infraestructura de Basis.WorkPlace.

Para configurar los ajustes para conectarse a un entorno remoto en la aplicación Basis.WorkPlace:

1. En el escritorio de Kaspersky Thin Client, haga clic en el botón **Basis.WorkPlace**.
2. Se abre una ventana para conectarse a un escritorio remoto. En la parte izquierda de esta ventana, haga clic en **Ajustes**.

Se abre una ventana donde puede configurar los ajustes que se usarán para redireccionar dispositivos al entorno remoto (vea la siguiente imagen).



Ventana para configurar la redirección de dispositivos a un entorno remoto desplegado en una infraestructura Basis.WorkPlace

3. Para configurar los ajustes de redirección de dispositivos a un entorno remoto:

- En el bloque de ajustes **Redirección de dispositivos USB**, seleccione los dispositivos que desea redirigir al entorno remoto: **Unidades de memoria USB y tarjetas inteligentes**, **Impresoras y otros dispositivos**.
- Si su estación de trabajo tiene dos monitores y desea que la imagen del escritorio remoto se muestre en ambos, marque la casilla **Usar dos monitores** en el bloque **Administración de monitores**.
- En el bloque de ajustes **Redirección de dispositivos de audio**, seleccione los dispositivos que se redirigirán al entorno remoto: **Dispositivos de reproducción de audio**, **Micrófono**.
- El volumen del audio y otros ajustes se controlan desde el entorno remoto.

El administrador de Basis.WorkPlace puede no permitir la redirección de dispositivos USB al escritorio remoto administrado por Basis.WorkPlace.

4. Para configurar los ajustes para conectarse a un entorno remoto geodistribuido, vaya a la pestaña **Ajustes de conexión** (vea la figura a continuación).

Para obtener una descripción detallada de los ajustes de esta pestaña, consulte la [Guía de instalación geodistribuida](#) en el sitio web de Basis.WorkPlace.

Haga lo siguiente en la pestaña seleccionada:

- En la sección **Direcciones de Administrador de conexiones**, haga clic en + y especifique la dirección IP del [agente](#) Basis.WorkPlace en el campo que se muestra. No puede agregar más de cuatro direcciones IP.

- b. En el campo **Número de intentos de reconexión**, ingrese la cantidad de veces que Kaspersky Thin Client intentará reconectarse al agente de Basis.WorkPlace si la conexión se interrumpe. El máximo admisible es de cinco intentos de reconexión.
- c. En la lista desplegable **Perfil de conexión**, seleccione el tipo de conexión que exista entre Kaspersky Thin Client y el agente de Basis.WorkPlace. El tipo de conexión depende de la velocidad de conexión. Los valores disponibles son los siguientes:
- Detectar automáticamente
 - Módem
 - Conexión de banda ancha de baja velocidad
 - Satélite
 - Conexión de banda ancha de alta velocidad
 - Red de área extensa
 - Red de área local



Ventana para configurar una conexión a un entorno remoto geodistribuido desplegado en una infraestructura de Basis.WorkPlace

5. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.
6. Haga clic en la flecha hacia atrás ubicada en la esquina superior derecha de la ventana para regresar a la ventana de conexión al entorno remoto.

Configurar el acceso a los ajustes de Kaspersky Thin Client

Puede configurar la interfaz de Kaspersky Thin Client para mostrar u ocultar los ajustes que haya configurado una vez y que no se requieran para el uso cotidiano del cliente ligero.

Cuando un cliente ligero forma parte de un [grupo de administración](#), los valores de los ajustes se pueden imponer a través de Web Console. Los ajustes fijados de este modo no se pueden configurar mediante la interfaz de Kaspersky Thin Client; tampoco es posible definir si tales ajustes se mostrarán en la interfaz o no.

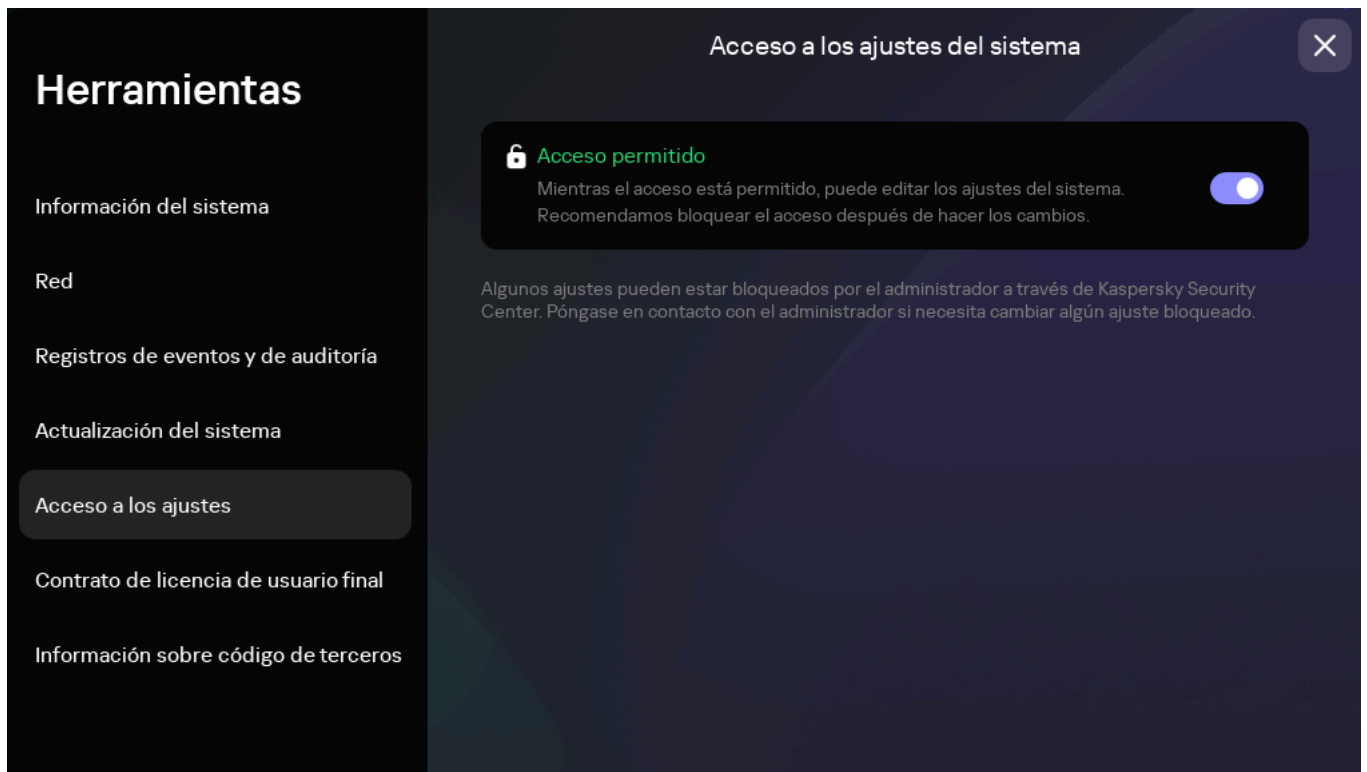
Para mostrar u ocultar los ajustes de Kaspersky Thin Client:

1. En el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Herramientas**.
2. En la ventana que se abre, elija la sección **Acceso a los ajustes** (vea la imagen de más abajo) y realice una de las siguientes acciones:
 - Si desea ocultar los ajustes, ponga el interruptor en la posición **Acceso bloqueado**.

Los siguientes ajustes dejarán de mostrarse en la interfaz del cliente ligero:

- [Ajustes de conexión RDP](#)
- [Ajustes de conexión a Basis.WorkPlace:](#)
- [Ajustes generales](#)
- [Ajustes de la red](#)
- [Ajustes de conexión a Kaspersky Security Center](#)
- [Fecha y hora](#)
- [Ajustes de ahorro de energía](#)
- [Disposición de los monitores](#)
- [Restablecimiento de los ajustes de Kaspersky Thin Client](#)

- Si desea mostrar los ajustes, ponga el interruptor en la posición **Acceso permitido**.
Se mostrarán los ajustes. Podrá asignarles nuevos valores.



Herramientas. Sección Acceso a los ajustes

Administrar Kaspersky Thin Client en un cliente ligero

Esta sección describe el principal escenario de funcionamiento de Kaspersky Thin Client y contiene instrucciones para usar Kaspersky Thin Client.

Escenario: trabajar en Kaspersky Thin Client en un cliente ligero

Las principales etapas para utilizar Kaspersky Thin Client en un [cliente ligero](#) son las siguientes:

1 Poner Kaspersky Thin Client en condiciones de iniciarse

Conecte los [periféricos](#) al cliente ligero antes de encenderlo por primera vez.

2 Iniciar Kaspersky Thin Client

[Encienda](#) el cliente ligero para comenzar.

3 Comenzar a trabajar con una sesión remota

[Conéctese a un entorno remoto](#) y comience a trabajar en una sesión remota.

4 Bloquear y desbloquear una sesión remota

[Bloquee su sesión remota](#) si necesita alejarse momentáneamente de la estación de trabajo. Continúe trabajando cuando regrese.

5 Cerrar la conexión remota

[Termine la sesión remota](#) cuando termine de trabajar.

6 Apagar Kaspersky Thin Client

Apague el cliente ligero cuando termine la jornada.

Conexión a un entorno remoto

En esta sección, se brinda información para conectarse a un [entorno remoto](#) utilizando las aplicaciones de Kaspersky Thin Client y para comenzar a trabajar en una [sesión remota](#).

Se aplican las siguientes limitaciones cuando se conecta a un entorno remoto en Kaspersky Thin Client:

- No es compatible el intercambio de archivos entre Kaspersky Thin Client y el entorno remoto.
- No es compatible el uso compartido del portapapeles entre Kaspersky Thin Client y el entorno remoto.
- No se admite la ejecución simultánea de varias sesiones remotas ni la conexión simultánea a varios entornos remotos dentro de una sola sesión remota.

Kaspersky Thin Client utiliza cifrado [TLS](#) (versiones 1.2 y 1.3) para proteger las sesiones remotas e impedir que los datos sean interceptados o suplantados.

Kaspersky Thin Client admite las siguientes suites de cifrado para conectarse a entornos remotos que ejecutan Microsoft Windows:

- Para 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}.
- Para 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}.

Conectarse a un entorno remoto usando la aplicación RDP

En la aplicación RDP, puede conectarse a [escritorios remotos](#) y [aplicaciones virtuales](#) mediante el protocolo RDP.

Conexión a un escritorio remoto

Para conectarse a un escritorio virtual en la aplicación RDP:

1. [Encienda Kaspersky Thin Client.](#)
2. En el escritorio de Kaspersky Thin Client, haga clic en el botón **RDP**.
3. En la ventana que se abre, ingrese los ajustes de conexión:
 - a. En el campo **Servidor**, ingrese la dirección IP o el nombre del servidor del Agente de conexión a Escritorio remoto de Microsoft.Kaspersky Thin Client guardará la dirección del último servidor con el que se establezca correctamente una conexión, por lo que no necesitará ingresar este dato nuevamente cuando quiera volver a conectarse.

b. En el campo **Nombre de usuario**, ingrese un nombre de usuario local o de dominio. Para indicar un nombre de usuario de dominio, puede usar el formato Dominio\Nombre de usuario o el formato Nombre de usuario.

Kaspersky Thin Client guardará el último nombre de usuario con el que se establezca correctamente una conexión al servidor, por lo que no necesitará ingresar este dato nuevamente cuando quiera volver a conectarse.

c. En el campo **Contraseña**, ingrese la contraseña del usuario.

Si no [activó la función de conexión automática](#), la contraseña no se guarda, y debe ingresarla nuevamente la próxima vez que se conecte.

4. Para [configurar los ajustes](#) para conectarse a un escritorio remoto, haga clic en **Ajustes** en la parte izquierda de la ventana.

5. Presione **Entrar** o haga clic en **Conectarse**.

Verá una ventana donde se le pedirá que agregue un certificado al sistema para que pueda conectarse al entorno remoto si se cumplen las siguientes condiciones:

- Se está conectando a un entorno remoto en la interfaz de Kaspersky Thin Client por primera vez.
- El cliente ligero se encuentra en uno de los siguientes estados:
 - No conectado a Kaspersky Security Center.
 - No agregado al [grupo de administración](#).
 - [No se han agregado certificados para conectarse al entorno remoto](#) para el grupo de administración al que pertenece el cliente ligero.

Verifique la configuración del certificado y haga clic en el botón **Agregar certificado**. El certificado se agregará al almacén de certificados del sistema de Kaspersky Thin Client y se usará en las subsiguientes conexiones.

6. Si, al [configurar una conexión de escritorio remoto](#), ingresó un id. de colección del Agente de conexión a Escritorio remoto y tiene acceso a más de un escritorio, cuando se abra la ventana para seleccionar un escritorio remoto, haga clic en el botón con el nombre del escritorio al que desee conectarse.

Se abre una ventana con el escritorio remoto y comienza la sesión remota.

Conexión a una aplicación virtual

Para conectarse a una [aplicación virtual](#) en la aplicación RDP:

1. [Encienda Kaspersky Thin Client](#).

2. En el escritorio de Kaspersky Thin Client, haga clic en el botón **RDP**.

3. En la ventana que se abre, ingrese los ajustes de conexión:

a. En el campo **Servidor**, ingrese la dirección IP o el nombre del servidor del Agente de conexión a Escritorio remoto de Microsoft.

Kaspersky Thin Client guardará la dirección del último servidor con el que se establezca correctamente una conexión, por lo que no necesitará ingresar este dato nuevamente cuando quiera volver a conectarse.

b. En el campo **Nombre de usuario**, ingrese un nombre de usuario local o de dominio. Para indicar un nombre de usuario de dominio, puede usar el formato Dominio\Nombre de usuario o el formato Nombre de usuario.

Kaspersky Thin Client guardará el último nombre de usuario con el que se establezca correctamente una conexión al servidor, por lo que no necesitará ingresar este dato nuevamente cuando quiera volver a conectarse.

c. En el campo **Contraseña**, ingrese la contraseña del usuario.

Si no [activó la función de conexión automática](#), la contraseña no se guarda, y debe ingresarla nuevamente la próxima vez que se conecte.

4. Haga clic en **Ajustes** en la parte izquierda de la ventana.

5. En el campo **Id. de colección del Agente de conexión a Escritorio remoto**, ingrese el id. de colección en formato `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` se refiere al identificador específico de la colección).

6. En el campo **Alias de la aplicación**, ingrese el alias de la aplicación virtual que desee abrir.

Kaspersky Thin Client guardará el último alias ingresado, por lo que no necesitará ingresar este dato nuevamente cuando quiera volver a conectarse.

7. Haga clic en la flecha hacia atrás en la esquina superior derecha de la ventana para regresar a la ventana de conexión.

8. En la ventana de conexión, presione **Entrar** o haga clic en **Conectarse**.

Verá una ventana donde se le pedirá que agregue un certificado al sistema para que pueda conectarse al entorno remoto si se cumplen las siguientes condiciones:

- Se está conectando a un entorno remoto en la interfaz de Kaspersky Thin Client por primera vez.
- El cliente ligero se encuentra en uno de los siguientes estados:
 - No conectado a Kaspersky Security Center.
 - No agregado al [grupo de administración](#) .
 - [No se han agregado certificados para conectarse al entorno remoto](#) para el grupo de administración al que pertenece el cliente ligero.

Verifique la configuración del certificado y haga clic en el botón **Agregar certificado**. El certificado se agregará al almacén de certificados del sistema de Kaspersky Thin Client y se usará en las subsiguientes conexiones.

Se abre una ventana con la aplicación virtual y comienza la sesión remota.

Para pasar a otra ventana de una aplicación virtual en ejecución,

pase el mouse sobre el ícono de la aplicación en el [panel de conexión](#) ubicado en la parte superior de la pantalla y, en la lista desplegable, seleccione la ventana de su interés.

Conectarse a un entorno remoto usando la aplicación Basis.WorkPlace

En la aplicación Basis.WorkPlace, puede conectarse a los escritorios virtualizados de Basis.WorkPlace.

Los usuarios no pueden iniciar un cambio de contraseña en Kaspersky Thin Client.

Para conectarse a un escritorio virtual en la aplicación Basis.WorkPlace:

1. [Encienda Kaspersky Thin Client.](#)

2. En el escritorio de Kaspersky Thin Client, haga clic en el botón **Basis.WorkPlace**.

3. En la ventana de conexión que se abre, ingrese los ajustes para conectarse a Basis.WorkPlace:

a. En el campo **Servidor**, especifique la dirección IP o el nombre del servidor [agente](#) de Basis.WorkPlace.

Kaspersky Thin Client guarda la dirección del último agente de Basis.WorkPlace con el que se haya establecido una conexión, así que no necesitará ingresar este dato nuevamente para volver a conectarse.

b. En el campo **Dominio**, ingrese el nombre del dominio.

c. En el campo **Nombre de usuario**, ingrese el nombre de usuario.

Kaspersky Thin Client guardará el último nombre de usuario con el que se establezca correctamente una conexión a Basis.WorkPlace, por lo que no necesitará ingresar este dato nuevamente para volver a conectarse.

d. En el campo **Contraseña**, ingrese la contraseña del usuario.

La contraseña del usuario no se guardará: deberá ingresarla de nuevo cuando desee volver a conectarse.

Si ingresa una contraseña incorrecta más veces de lo permitido, la cuenta de usuario se bloqueará. Si esto sucede, se mostrará un mensaje al respecto en la ventana de conexión al escritorio virtual. El administrador de Basis.WorkPlace determina, a través de la directiva de seguridad activa, el máximo de veces que se permite ingresar una contraseña errónea.

4. Presione **Entrar** o haga clic en **Conectarse**.

Verá una ventana donde se le pedirá que agregue un certificado al sistema para que pueda conectarse al entorno remoto si se cumplen las siguientes condiciones:

- Se está conectando a un entorno remoto en la interfaz de Kaspersky Thin Client por primera vez.
- El cliente ligero se encuentra en uno de los siguientes estados:
 - No conectado a Kaspersky Security Center.
 - No agregado al [grupo de administración](#).
 - [No se han agregado certificados para conectarse al entorno remoto](#) para el grupo de administración al que pertenece el cliente ligero.

Verifique la configuración del certificado y haga clic en el botón **Agregar certificado**. El certificado se agregará al almacén de certificados del sistema de Kaspersky Thin Client y se usará en las subsiguientes conexiones.

Se abrirá una ventana de la infraestructura de Basis.WorkPlace con los escritorios virtuales disponibles.

5. Si desea actualizar la lista de escritorios virtuales, haga clic en el botón **Recargar**.

6. Haga clic en el botón con el nombre del escritorio virtual al que desee conectarse.

Aparecerá una ventana con el escritorio virtual. Comenzará una sesión remota.

El administrador puede imponer restricciones que limiten el acceso de un usuario a Basis.WorkPlace. Entre otras acciones, el administrador puede bloquear la cuenta del usuario o quitarle la posibilidad de usar escritorios virtuales que antes estaban disponibles para su cuenta de usuario. Si tiene problemas para conectarse a un entorno remoto, comuníquese con el administrador de su organización.

Conectarse a un entorno remoto usando la aplicación Web Access

En la aplicación Web Access, puede conectarse a un entorno remoto desplegado en infraestructuras Citrix Workspace. Web Access admite HTML5 y proporciona una conexión HTTPS segura al conectarse.

Los datos necesarios para la conexión remota (por ejemplo, los archivos cookies) se conservarán en el cliente ligero hasta que se cierre la conexión remota. Los datos se eliminarán una vez que finalice la conexión.

Para conectarse a un entorno remoto usando la aplicación Web Access:

1. [Encienda Kaspersky Thin Client](#).

2. En el escritorio de Kaspersky Thin Client, haga clic en el botón **Web Access**.

3. En la ventana de conexión que se abre, introduzca la dirección del servidor de entorno remoto requerida en el campo **Servidor**.

4. Presione **Entrar** o haga clic en **Conectarse**.

Verá una ventana donde se le pedirá que agregue un certificado al sistema para que pueda conectarse al entorno remoto si se cumplen las siguientes condiciones:

- Se está conectando a un entorno remoto en la interfaz de Kaspersky Thin Client por primera vez.
- El cliente ligero se encuentra en uno de los siguientes estados:
 - No conectado a Kaspersky Security Center.
 - No agregado al [grupo de administración](#) .
 - [No se han agregado certificados para conectarse al entorno remoto](#) para el grupo de administración al que pertenece el cliente ligero.

Verifique la configuración del certificado y haga clic en el botón **Agregar certificado**. El certificado se agregará al almacén de certificados del sistema de Kaspersky Thin Client y se usará en las subsiguientes conexiones.

Se muestra la ventana para ingresar los datos de conexión.

5. Ingrese el nombre de usuario y la contraseña para conectarse al entorno remoto.

El sistema no guarda las credenciales para conectarse a un entorno remoto implementado en una infraestructura de Citrix Workspace, por lo que debe ingresarlas cada vez que inicie una sesión remota.

Si tiene un escritorio remoto disponible, se lo mostrará en la pantalla y podrá comenzar a trabajar en el entorno remoto. Si tiene varios escritorios remotos, verá una ventana con una lista de ellos.

6. Si desea actualizar la lista de escritorios remotos, haga clic en el botón **Recargar**.

7. Haga clic en el botón con el nombre del escritorio remoto al que desee conectarse.

Aparecerá una ventana del entorno remoto al que se haya conectado. Comenzará una [sesión remota](#).

Controlar una sesión remota

En esta sección, se explica cómo controlar una [sesión remota](#) mediante la interfaz de Kaspersky Thin Client utilizando las [teclas de acceso rápido](#) y el panel de conexión.

Utilizar el panel de conexión

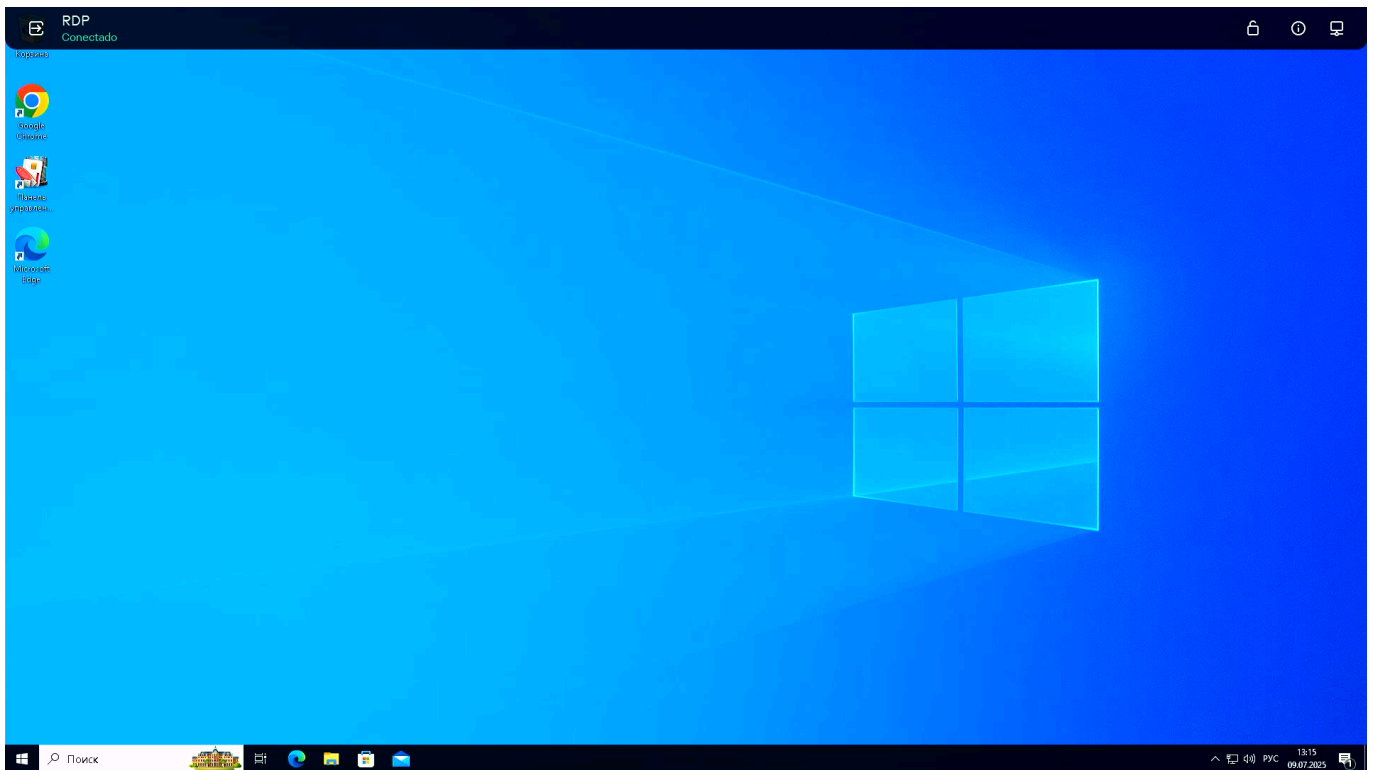
El panel de conexión (también denominado más adelante "el panel") aparece en la parte superior de la pantalla después de conectarse correctamente a un entorno remoto. Se utiliza para controlar la [sesión remota](#) activa.

Estados del panel de conexión

El panel de conexión puede encontrarse en uno de los siguientes estados:

- Ampliado.

El panel se muestra completamente en la parte superior de la pantalla de sesión remota (consulte la imagen a continuación).



Ventana que muestra una sesión remota en ejecución con el panel de conexión ampliado

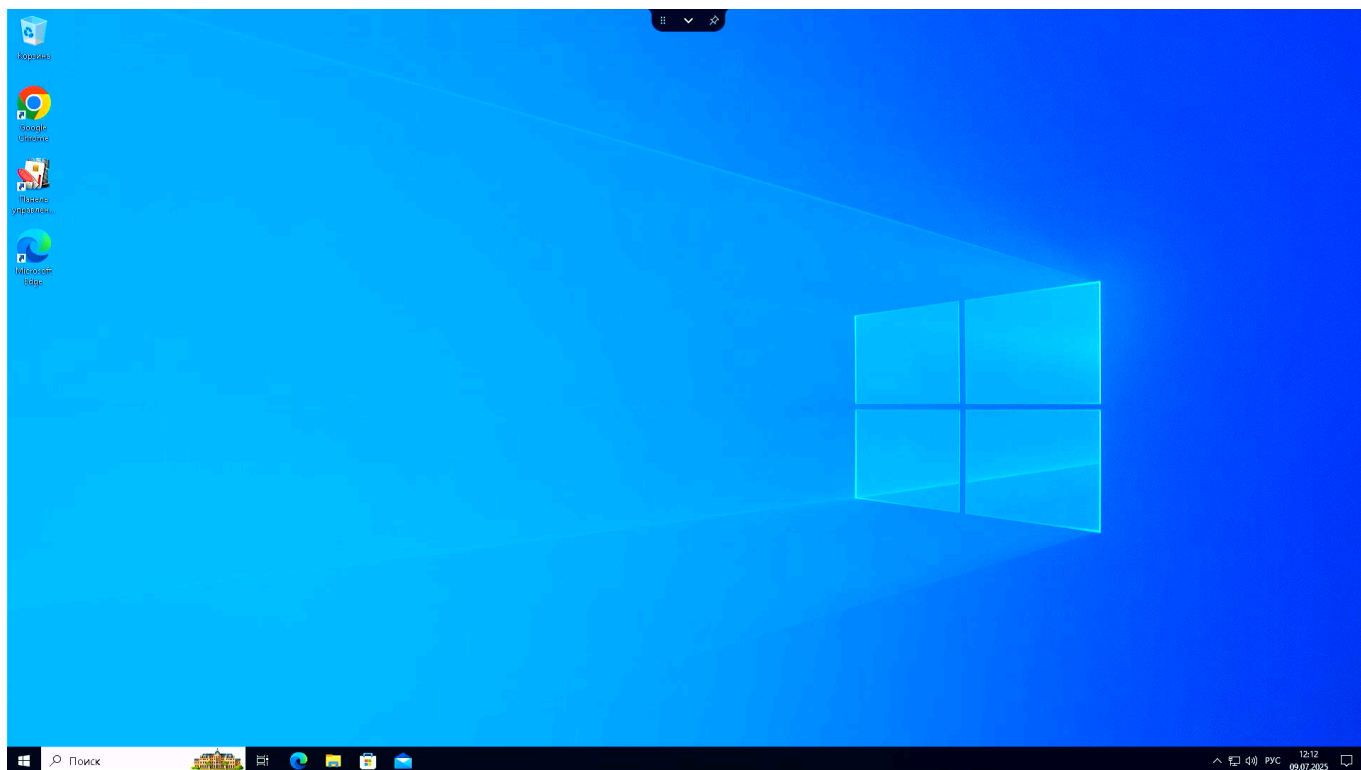
- Oculto.

El panel no se muestra en la pantalla.

Si el panel de conexión no está fijado, se contrae automáticamente cuando deja de estar enfocado por el teclado o el mouse.

- Contraído.

Los elementos de control del panel de conexión se muestran cuando se coloca el cursor en la parte superior de la pantalla (consulte la imagen a continuación).



Ventana que muestra una sesión remota en ejecución con el panel de conexión contraído

Cambio del estado del panel de conexión

En la interfaz de Kaspersky Thin Client, se puede cambiar el estado del panel de conexión. También se puede mover el panel contraído de manera horizontal y fijarlo en cualquier lugar de la pantalla.

Puede cambiar el estado del panel de conexión de la siguiente manera:

- Si desea ocultar completamente el panel de conexión contraído, realice una de las siguientes acciones:
 - Presione **CTRL+ALT+HOME** o **ESC**.
 - Haga clic en cualquier otra parte de la pantalla fuera del panel.
- Si desea mostrar un panel de conexión contraído, coloque el cursor sobre la parte superior de la pantalla. Se mostrarán los elementos de control del panel.
- Si desea ampliar el panel de conexión, realice una de las siguientes acciones:
 - Presione **CTRL+ALT+HOME**.
 - Restablezca el panel de conexión contraído y haga clic en el botón .

Puede administrar un panel de conexión minimizado de las siguientes maneras:

- Si desea cambiar la posición del panel, haga clic y mantenga presionado el botón  para mover el panel hacia la izquierda o hacia la derecha.
- Si desea fijar un panel contraído en su posición actual, haga clic en el botón .
El panel de conexión se mostrará contraído en la parte superior de la pantalla hasta que decida ocultarlo o dejar de tenerlo fijado.
- Si tiene que dejar de tener fijado el panel, haga clic en el botón .

La posición del panel contraído en la pantalla queda guardada para conexiones futuras, incluso después de reiniciar o apagar el cliente ligero.

Bloquear y desbloquear una sesión remota

Kaspersky Thin Client bloquea automáticamente las sesiones remotas cuando la pantalla se oscurece después de un período de inactividad [definido en la configuración del cliente ligero](#). Las sesiones también se pueden bloquear y desbloquear en forma manual.

Para bloquear una sesión remota activa,

presione **Win+L** o [expanda el panel de conexión](#) y haga clic en .

La sesión remota se bloqueará. Se mostrará una pantalla de bloqueo.

Para cerrar una sesión remota bloqueada:

1. Mueva el mouse o presione alguna tecla.
2. En la pantalla que aparece, haga clic en **Cerrar la sesión remota**.

La sesión remota se cerrará y se mostrará la ventana de la aplicación que usó para iniciar la sesión remota.

Para desbloquear una sesión remota:

1. Mueva el mouse o presione alguna tecla.
2. En la pantalla que aparece, escriba la contraseña que utilizó para conectarse al sistema remoto.
Si se autenticó inicialmente usando un [agente](#) u otro servicio de conexión remota, deberá ingresar la contraseña que haya usado para conectarse a ese servicio.
3. Haga clic en **Desbloquear**.

La sesión remota se desbloqueará. Se mostrará la pantalla del entorno remoto.

Cerrar una sesión remota

Para cerrar una sesión remota,

[restablezca el panel de conexión](#) y haga clic en  o presione **CTRL+D**.

La sesión remota se cerrará y se mostrará una ventana de conexión.

Administrar dispositivos de reproducción y grabación de audio en el panel de conexiones

Puede utilizar un conector para miniclavija o un puerto USB para conectar varios dispositivos de grabación y reproducción de audio a un cliente ligero con Kaspersky Thin Client para redirigirlos al entorno remoto. [Puede cambiar entre los dispositivos conectados](#) mediante la interfaz de Kaspersky Thin Client.

El volumen del audio y otros ajustes se controlan desde el entorno remoto.

Cuando se accede un entorno remoto desplegado en la infraestructura Citrix Workspace, no es posible redirigir a un mismo tiempo más de dos dispositivos USB.

La conexión a través de un miniconector no es compatible con los clientes ligeros Dell Wyse 3040.

Para seleccionar los dispositivos de reproducción y grabación de audio que se usarán en una sesión remota:

1. [Restaure el panel de conexión](#) y haga clic en el botón  del mismo.
2. En la ventana que se abre, seleccione un dispositivo de reproducción de audio en la lista **Salida** y un dispositivo de grabación de audio en la lista **Entrada**.

Si el dispositivo que desea usar no está en la lista, revise los ajustes de redirección en la aplicación que haya usado para conectarse al entorno remoto o comuníquese con el administrador de su empresa.

Administrar ventanas de aplicaciones virtuales

Cuando se conecta a una [aplicación virtual](#), puede cambiar de ventana en el panel de conexión de Kaspersky Thin Client.

Para pasar a otra ventana de una aplicación virtual en ejecución:

1. Restablezca el panel de conexión.
2. Haga clic en el ícono de la aplicación.
Se mostrará una lista de ventanas con las aplicaciones abiertas.
3. Haga clic en la ventana correspondiente.
Se mostrará la ventana de la aplicación virtual seleccionada.

Web Access: redirigir dispositivos USB a un entorno remoto

Puede redireccionar impresoras, escáneres, cámaras web y unidades de memoria USB a un entorno remoto desplegado en una infraestructura de Citrix Workspace. La redirección de la cámara web no requiere configuración adicional en el entorno remoto.

No se pueden redireccionar más de dos [dispositivos USB](#) al mismo tiempo.

Redireccionar una impresora o un escáner a un entorno remoto

Para redireccionar una impresora o un escáner a un entorno remoto:

1. Conecte el dispositivo al cliente ligero mediante el conector USB.
2. Si está conectando un escáner, [especifique manualmente el tipo de dispositivo](#) en **Ajustes -> Dispositivos USB no identificados**.
3. [Conectarse a un entorno remoto en la aplicación Web Access](#).
4. Expanda el panel de control de Citrix Workspace en la parte superior de la ventana y haga clic en el botón **USB Devices**.
Verá una ventana que le pedirá que redirija el dispositivo USB.
5. Haga clic en **Agregar**.
Verá una ventana que muestra una lista de dispositivos disponibles para la redirección.
6. Si el dispositivo correspondiente no aparece en la lista, intente reiniciar la sesión remota sin quitar el dispositivo USB.
7. Seleccione el dispositivo correspondiente en la lista y haga clic en **Conectarse**.

El dispositivo se redireccionará al entorno remoto. Ahora puede usarlo en un escritorio remoto.

Si necesita redireccionar varios dispositivos, repita los pasos 4 a 6 de estas instrucciones para cada uno de ellos.

Para obtener más información sobre la redirección de dispositivos USB, consulte la [documentación del producto Citrix Workspace](#).

Redirigir dispositivos USB a un entorno remoto

También puede redireccionar las unidades de memoria USB al entorno remoto y luego quitarlas de manera segura. La redirección utiliza la tecnología Client Drive Mapping. Para obtener más detalles, consulte la [documentación del producto Citrix Workspace](#).

Para redireccionar las unidades de memoria USB a un entorno remoto desplegado en una infraestructura de Citrix Workspace:

1. Conecte el dispositivo al cliente ligero mediante el conector USB.
2. [Conectarse a un entorno remoto en la aplicación Web Access](#).
3. Expanda el panel de control de Citrix Workspace en la parte superior de la ventana y haga clic en **Map a drive**.
Verá la ventana para seleccionar el directorio de montaje.
4. Haga clic en **Browse**.
Se muestra una ventana de confirmación.
5. Haga clic en **Redireccionar** para confirmar la redirección de todas las unidades de memoria USB conectadas al cliente ligero.
Verá la ventana para seleccionar el directorio de montaje.
6. Haga clic en **Add** para confirmar la redirección.
7. Finalice la sesión remota y vuelva a conectarse al entorno remoto para completar la redirección.

Las unidades de memoria USB se redireccionarán al entorno remoto. Se mostrará un disco que contiene las carpetas con los nombres de las unidades de memoria USB redireccionadas en el sistema de archivos del entorno remoto.

Expulsión segura de dispositivos USB en una sesión remota

Kaspersky Thin Client admite la extracción segura de unidades de memoria USB en una sesión remota. Para evitar dañar los datos almacenados en el dispositivo, expulse el dispositivo de acuerdo con las siguientes instrucciones.

Para expulsar de forma segura una unidad de memoria USB en una sesión remota:

1. [Conectarse a un entorno remoto en la aplicación Web Access](#).
 2. [Restablezca el panel de conexión](#) y haga clic en el botón .
- Verá una lista de dispositivos USB que se han redirigido al entorno remoto.

3. Seleccione el dispositivo correspondiente o haga clic en **Expulsar todas las unidades de memoria USB**.
 4. Si hay un problema con la eliminación segura, se mostrará un mensaje de error. Cierre todas las ventanas del escritorio remoto y finalice los procesos de copia y vuelva a intentarlo.
- El dispositivo ahora está listo para ser quitado de manera segura y puede desconectarlo físicamente del cliente ligero.

Consultar información sobre Kaspersky Thin Client y un cliente ligero

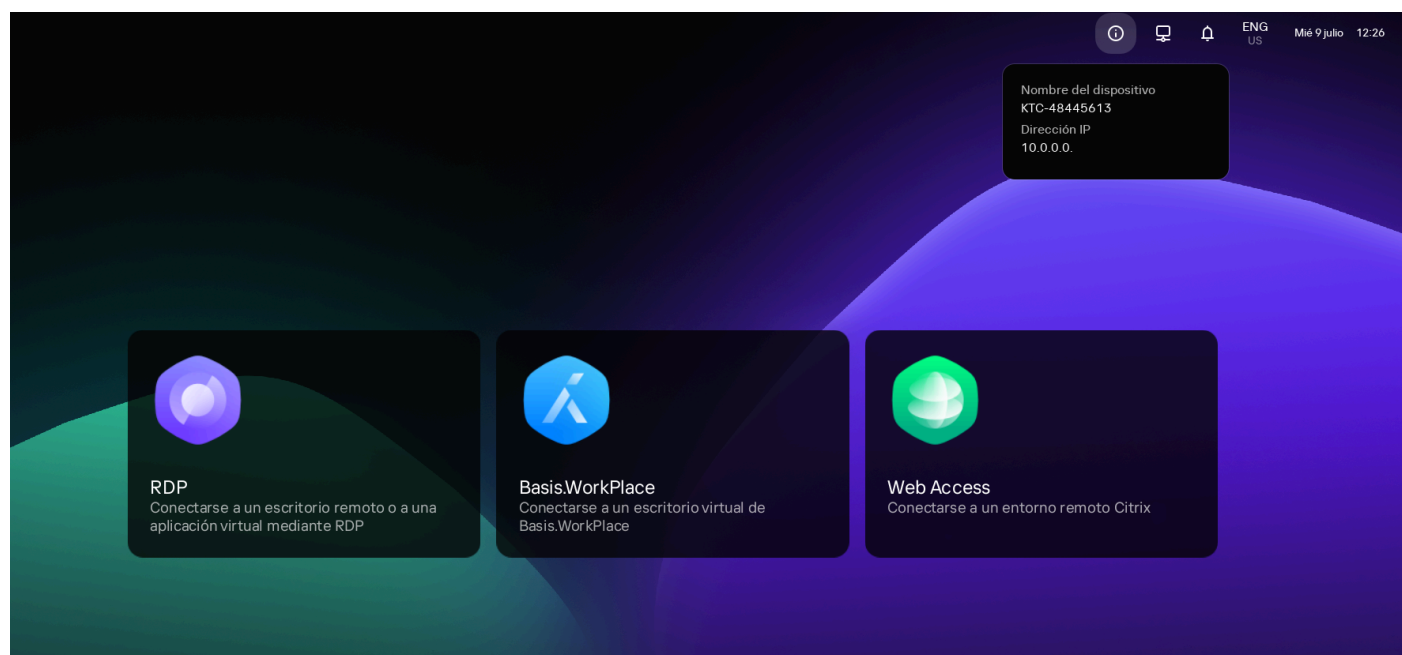
En la interfaz de Kaspersky Thin Client, puede ver la versión actual del sistema operativo, su fecha de lanzamiento, y la versión del SDK. La interfaz también muestra la dirección IP y el nombre del cliente ligero.

Para ver información sobre un cliente ligero,

en el panel de control de Kaspersky Thin Client, haga clic en .

Aparece una ventana que contiene información sobre el cliente ligero.

Esta ventana también mostrará los contactos del Servicio de soporte técnico o los contactos del administrador de su empresa si el cliente ligero está agregado al [grupo de administración](#) y si estos datos se [especificaron en la directiva a través de la Consola web](#).

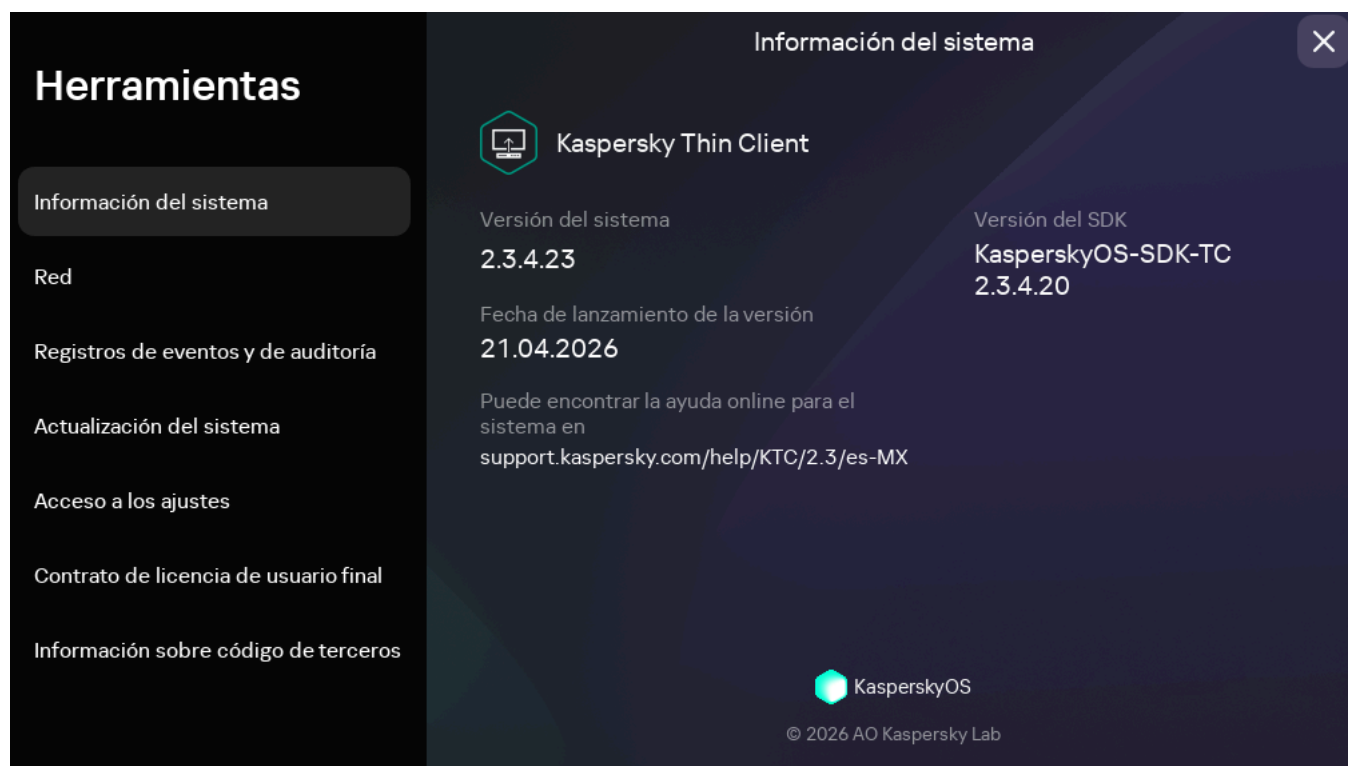


Ventana de información del cliente ligero

Para ver información sobre Kaspersky Thin Client,

en el panel de control de Kaspersky Thin Client, haga clic en , y, en el menú que se abre, seleccione **Herramientas → Información del sistema**.

Aparecerá una ventana con información sobre Kaspersky Thin Client.



Herramientas. Sección Información del sistema

Ver información sobre el estado de la red

En la interfaz de Kaspersky Thin Client, podrá ver la configuración para conectar el sistema a la red y ver información relacionada con el estado de conexión de la red. La información sobre los valores de la conexión de red de Kaspersky Thin Client se actualiza automáticamente al menos una vez por segundo.

Para ver la información sobre el estado de conexión de la red,

coloque el cursor sobre el ícono  en el panel de control de Kaspersky Thin Client.

Aparecerá una ventana con información sobre el estado de conexión de la red.

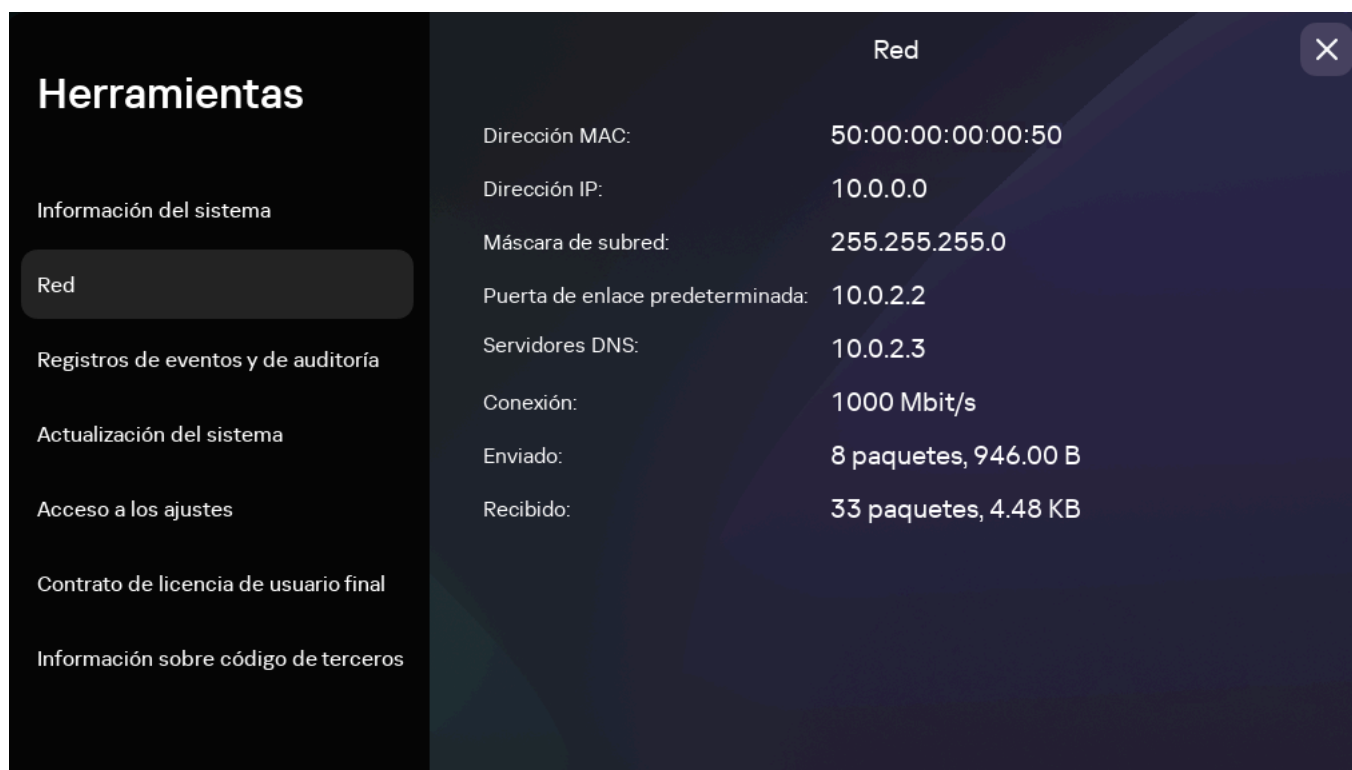
Para ver la configuración de la conexión de la red, siga estos pasos:

en el panel de control de Kaspersky Thin Client, haga clic en  y seleccione **Herramientas** → **Red** en el menú que se abre (consulte la imagen a continuación).

Aparecerá una ventana que muestra la configuración para conectar Kaspersky Thin Client a la red (consulte la imagen a continuación):

- **Dirección MAC:** la dirección MAC del dispositivo en el que se encuentra instalado Kaspersky Thin Client.
- **Dirección IP:** la dirección IP del dispositivo en el que se encuentra instalado Kaspersky Thin Client.
- **Máscara de subred:** la máscara de subred en la que está incluida la dirección IP del dispositivo.

- **Puerta de enlace predeterminada:** la dirección de la puerta de enlace de la red.
- **Servidores DNS:** las direcciones de los servidores DNS. Para ver todas las direcciones (si hay más de tres), pose el mouse sobre el valor de este parámetro.
- **Conexión:** el estado y la velocidad de la conexión de red de Kaspersky Thin Client.
- **Enviado:** la cantidad de paquetes de red enviados por Kaspersky Thin Client y el tamaño total de estos paquetes.
- **Recibido:** la cantidad de paquetes de red recibidos por Kaspersky Thin Client y el tamaño total de estos paquetes.



Herramientas. Sección Red

Ver notificaciones de Kaspersky Thin Client

La interfaz de Kaspersky Thin Client muestra los siguientes tipos de notificaciones:

- Solicitudes de seleccionar una acción haciendo clic en un botón, por ejemplo, ejecutar o aplazar una actualización. Después de un tiempo, Kaspersky Thin Client repetirá cualquier solicitud que haya cerrado sin seleccionar una acción. Una solicitud se considera resuelta después de que el usuario selecciona una acción.
- Solicitudes de ir a otra sección de Kaspersky Thin Client para configurar más ajustes. Por ejemplo, el sistema le pide al usuario que configure la disposición del monitor cuando conecta un segundo monitor. Puede elegir entre descartar la solicitud o hacer clic en el botón correspondiente para ir a la sección del otro sistema.
- Notificaciones informativas. Estas notificaciones no requieren que realice ninguna acción. Su única opción es cerrar la notificación después de leer su contenido.

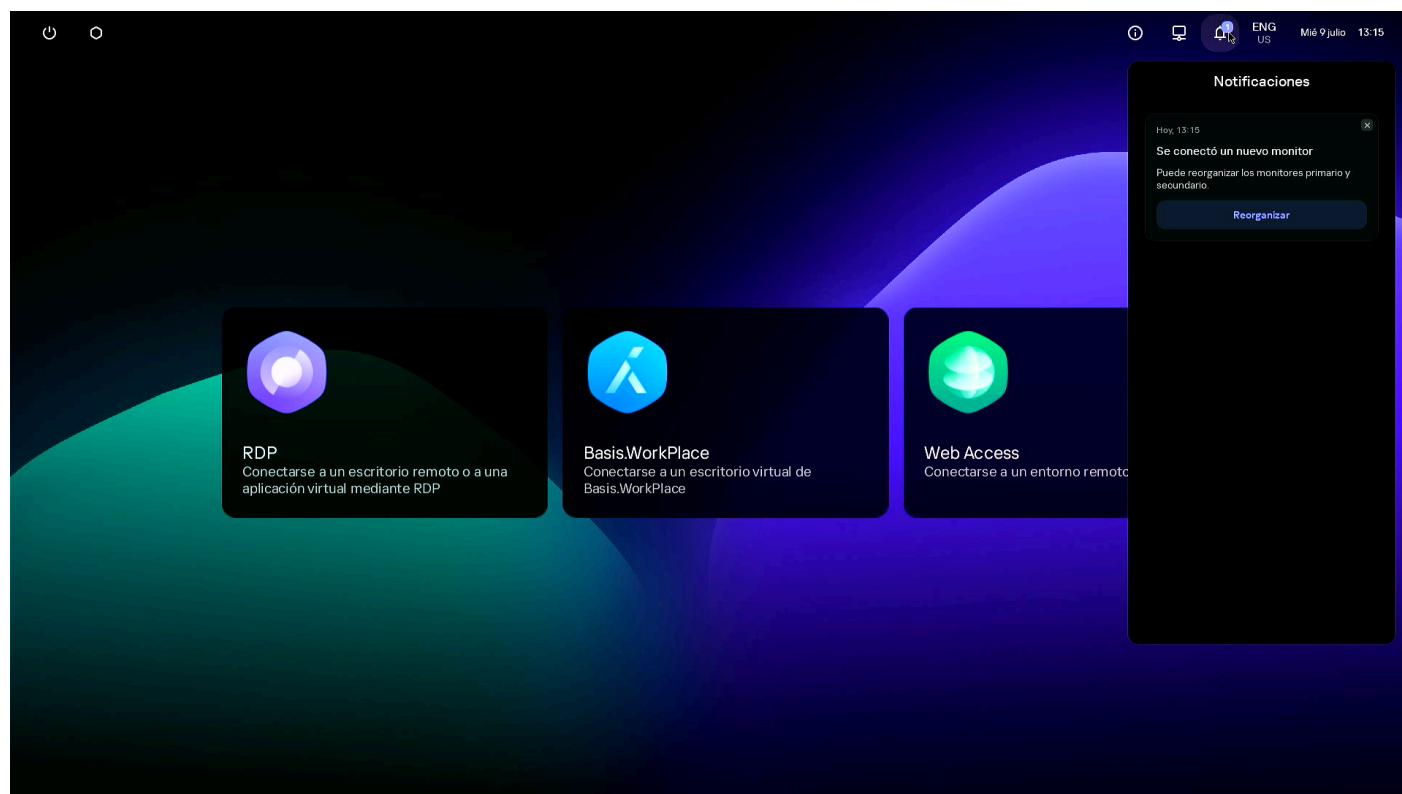
Si el cursor o el foco del teclado están fuera del área de notificación, las solicitudes no resueltas y no leídas se ocultan y el contador en el panel de control muestra su número.

Las notificaciones sobre actualizaciones no se ocultan de forma automática en las sesiones remotas. Para que desaparezcan, se las debe descartar manualmente o se debe realizar la acción solicitada.

Para ver una lista de todas las notificaciones de Kaspersky Thin Client:

En el [panel de control](#) de Kaspersky Thin Client, haga clic en .

Aparecerá el panel de notificaciones. Si tiene nuevas notificaciones, se mostrarán en el panel (vea la figura a continuación).



Panel de notificaciones de Kaspersky Thin Client

Administrar certificados en la interfaz de Kaspersky Thin Client

Kaspersky Thin Client no verifica si los certificados están en la lista de revocación de certificados.

Acerca de los certificados para conectarse a Kaspersky Security Center

Si el administrador de Kaspersky Security Center sustituye [el certificado de conexión a Kaspersky Security Center](#), en algunos casos se deberá confirmar la sustitución del certificado. Esta situación puede presentarse, por ejemplo, si el cliente ligero estuvo apagado durante mucho tiempo, no se sincronizó con Kaspersky Security Center y el certificado que se usó anteriormente para conectarse a Kaspersky Security Center caducó.

Para confirmar la sustitución del certificado para dispositivos móviles utilizado para conectarse a Kaspersky Security Center:

1. Encienda Kaspersky Thin Client.
2. Se abrirá una ventana llamada **Hay que reemplazar el certificado**. Memorice el código de confirmación que aparece en la ventana y proporciónesele al administrador de Kaspersky Security Center. Encontrará los datos de contacto del administrador en la ventana **Hay que reemplazar el certificado**. El administrador de Kaspersky Security Center le responderá con un código de sustitución del certificado.
3. Haga clic en **Siguiente**.
4. Se abrirá una ventana llamada **Código de sustitución del certificado**. Ingrese el código que le haya brindado el administrador de Kaspersky Security Center y haga clic en el botón **Confirmar**.

Como resultado, el nuevo certificado para conectarse a Kaspersky Security Center se guardará en el almacén de certificados de Kaspersky Thin Client y, de allí en más, se lo usará para conectarse a Kaspersky Security Center.

Acerca de los certificados utilizados para conectarse a un entorno remoto y a un servidor de registros

Si un cliente ligero no está conectado a Kaspersky Security Center y el administrador no le ha asignado certificados en Web Console, quien utilice ese dispositivo podrá conectarse a nodos y usar certificados que no estén controlados por el administrador. Recomendamos configurar la [conexión de un grupo de administración](#) a un servidor de registros y a un entorno remoto exclusivamente mediante certificados asignados por el administrador en la Consola web. Estas medidas ayudará a evitar que Kaspersky Thin Client se conecte a nodos que no sean de confianza.

Puede usar o rechazar un certificado en la interfaz de Kaspersky Thin Client en las siguientes situaciones:

- [Al conectar Kaspersky Thin Client a Kaspersky Security Center por primera vez.](#)
- Al conectarse por primera vez a un entorno remoto.
- [Al conectarse por primera vez a un servidor de registros.](#)

Los certificados aceptados se guardan en el almacén del sistema de Kaspersky Thin Client.

Si un cliente ligero forma parte de un [grupo de administración](#) para el que se han [asignado certificados a través de Web Console](#), no es posible administrar los certificados mediante la interfaz de Kaspersky Thin Client.

Administrar Kaspersky Thin Client mediante combinaciones de teclas

Puede utilizar atajos de teclado dedicados para interactuar con Kaspersky Thin Client o con una [sesión remota](#). La siguiente tabla enumera todas las teclas de acceso rápido y combinaciones de teclas disponibles.

Teclas y combinaciones de teclas	Acciones
Windows	Abrir o cerrar el menú de apagado .
→ ←	Alternar entre las aplicaciones disponibles en el escritorio de Kaspersky Thin Client (RDP , Basis.WorkPlace y Web Access).
↑ ↓	• Escoger entre los elementos de la lista desplegable. • Desplazar el contenido de la página hacia arriba o hacia abajo.
Tabulador	Desplazarse de <i>izquierda a derecha</i> o de <i>arriba abajo</i> entre los siguientes elementos: • Opciones de conexión. • El orden de los campos en, por ejemplo, la ventana Ajustes. • Botones del panel de conexión. Al moverse entre los elementos, se omiten los elementos no disponibles, como los campos deshabilitados y los elementos inactivos.
Mayús + Tabulador	Desplazarse de <i>derecha a izquierda</i> o de <i>abajo arriba</i> entre los siguientes elementos: • Opciones de conexión. • El orden de los campos en, por ejemplo, la ventana Ajustes. • Botones del panel de conexión. Al moverse entre los elementos, se omiten los elementos no disponibles, como los campos deshabilitados y los elementos inactivos.
Espacio o Intro	• Hacer clic en el botón en el que se encuentre el foco del teclado. • Abrir o cerrar la lista desplegable en la que se encuentre el foco del teclado. Al moverse entre los elementos, se omiten los elementos no disponibles, como los campos deshabilitados y los elementos inactivos.
Esc	• Cerrar la ventana activa. • Contraer el panel de conexión cuando tenga el foco del teclado.
Alt + Mayús	Cambiar el idioma del teclado.
Alt + Retroceder página Alt + Avanzar página	Pasar a la sección anterior o siguiente en las ventanas Ajustes y Herramientas. Cuando cambia entre las secciones, su estado y el elemento en foco se conservan. Por ejemplo, en la ventana Ajustes, cuando cambia de la sección General a la sección Red, el foco en la sección General permanece en el mismo campo donde estaba cuando cambió a otra sección.
Ctrl+Alt+Inicio	Contraer o restaurar el panel de conexión .
Ctrl+D	Cerrar la sesión remota. Este acceso directo solo puede utilizarse si el panel de conexión se ha expandido.
Win+ 	Abrir Ajustes desde el escritorio de Kaspersky Thin Client si el acceso a los ajustes no se ha bloqueado .
Win+U	Abrir Herramientas desde el escritorio de Kaspersky Thin Client.
Win + L	Bloquear una sesión remota activa.
Win+Esc	Apagar Kaspersky Thin Client desde el escritorio de Kaspersky Thin Client.
Win+F12 o Win+Fin	Reiniciar Kaspersky Thin Client desde el escritorio de Kaspersky Thin Client.
Win+A o Win+N	Abrir el panel de notificaciones desde el escritorio de Kaspersky Thin Client.
Win+↓ Win+↑	Contraer o restaurar una ventana mientras se está conectado a una aplicación virtual.
Win+M	Minimizar todas las ventanas mientras se está conectado a una aplicación virtual.
Win+Mayús+M	Restaurar todas las ventanas mientras se está conectado a una aplicación virtual.

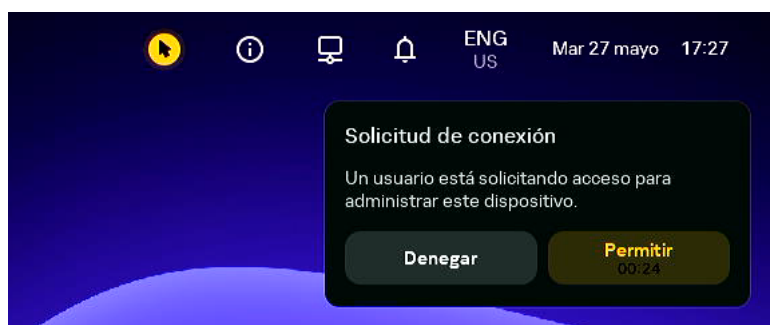
Controlar el acceso a la capacidad de administración remota y a la pantalla del entorno remoto

En Kaspersky Thin Client, se pueden aceptar y rechazar las solicitudes de acceso a la administración remota del cliente ligero y de acceso a la pantalla de la [sesión remota](#) con la que esté trabajando (en adelante también denominada la "pantalla de entorno remoto").

Para aceptar o denegar una solicitud de administración remota o una solicitud de acceso a la pantalla del entorno remoto:

1. [Encienda el cliente ligero](#) y asegúrese de que [el dispositivo esté conectado a la red](#).

Cuando intente conectarse a Kaspersky Thin Client, se mostrará el ícono  en el panel de control. En el escritorio, aparecerá una notificación que le solicitará conexión (consulte la imagen a continuación).



Notificación de escritorio de Kaspersky Thin Client que contiene una solicitud para la administración remota del cliente ligero.

2. Realice una de las siguientes acciones:

- Haga clic en **Denegar** para que Kaspersky Thin Client no tenga acceso a la administración remota.
- Haga clic en **Permitir** para permitir que el administrador vea la pantalla de Kaspersky Thin Client y administre la configuración del sistema.

Solo acepte la solicitud si está seguro de que el administrador de su empresa es la persona que se está conectando a Kaspersky Thin Client.

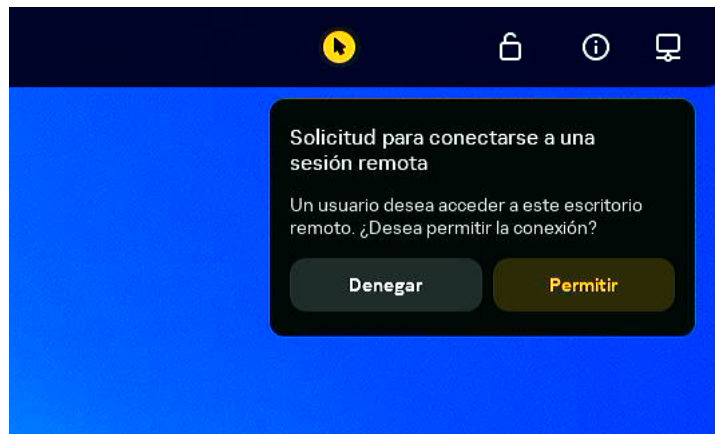
La administración de Kaspersky Thin Client se transferirá al administrador.

Si se estableció el modo **Permitir automáticamente** [para un dispositivo](#) o [su grupo de administración](#) en la [configuración de Kaspersky Thin Client](#) o en la configuración de administración remota de Web Console, y no hay respuesta a la solicitud dentro de los 30 segundos, la administración de Kaspersky Thin Client se transfiere automáticamente al administrador.

3. Si se está ejecutando una [sesión remota](#) en Kaspersky Thin Client al momento de la conexión remota o si el administrador inicia una sesión remota durante la administración remota del dispositivo, el acceso a la pantalla de dicha sesión remota se regula de la siguiente manera:

- Si se permite la conexión automática a la pantalla remota [para el dispositivo](#) o [su grupo de administración](#) en la [configuración de Kaspersky Thin Client](#) o en la configuración de administración remota en Web Console, el administrador tiene acceso automáticamente a la pantalla de la sesión remota que se está ejecutando.
- Si el modo de acceso a la pantalla del entorno remoto se estableció en **Permitir caso por caso** en la configuración de Kaspersky Thin Client o en la configuración de administración remota en Web Console, se mostrará una notificación que contiene una solicitud para conectarse a la sesión remota en la interfaz de Kaspersky Thin Client (consulte la imagen a continuación).

La administración de Kaspersky Thin Client se transferirá automáticamente al usuario.



Notificación que contiene una solicitud de conexión de sesión remota

4. Realice una de las siguientes acciones:

- Haga clic en **Denegar** para impedir que el administrador acceda a la pantalla del entorno remoto.
Si desea que el administrador recupere el control administrativo del cliente ligero, pero no quiere darle acceso a la pantalla del entorno remoto, [cierre la sesión remota](#).
- Haga clic en **Permitir** para que el administrador pueda ver la pantalla del entorno remoto y administrar la sesión remota.

La administración de Kaspersky Thin Client se transferirá al administrador.

Conexión remota a un cliente ligero

El administrador puede usar un cliente de RDP instalado en su dispositivo para conectarse a un cliente ligero remoto y resolver problemas a distancia o ayudar al usuario a configurar Kaspersky Thin Client.

Para que la administración remota funcione, el cliente ligero debe estar [encendido](#) y [conectado a la red](#). El modo de acceso a la administración remota **Permitir automáticamente** o **Permitir caso por caso** debe estar configurado para el [cliente ligero](#) o [su grupo de administración](#) en la [configuración de Kaspersky Thin Client](#) o en la configuración de administración remota de Web Console.

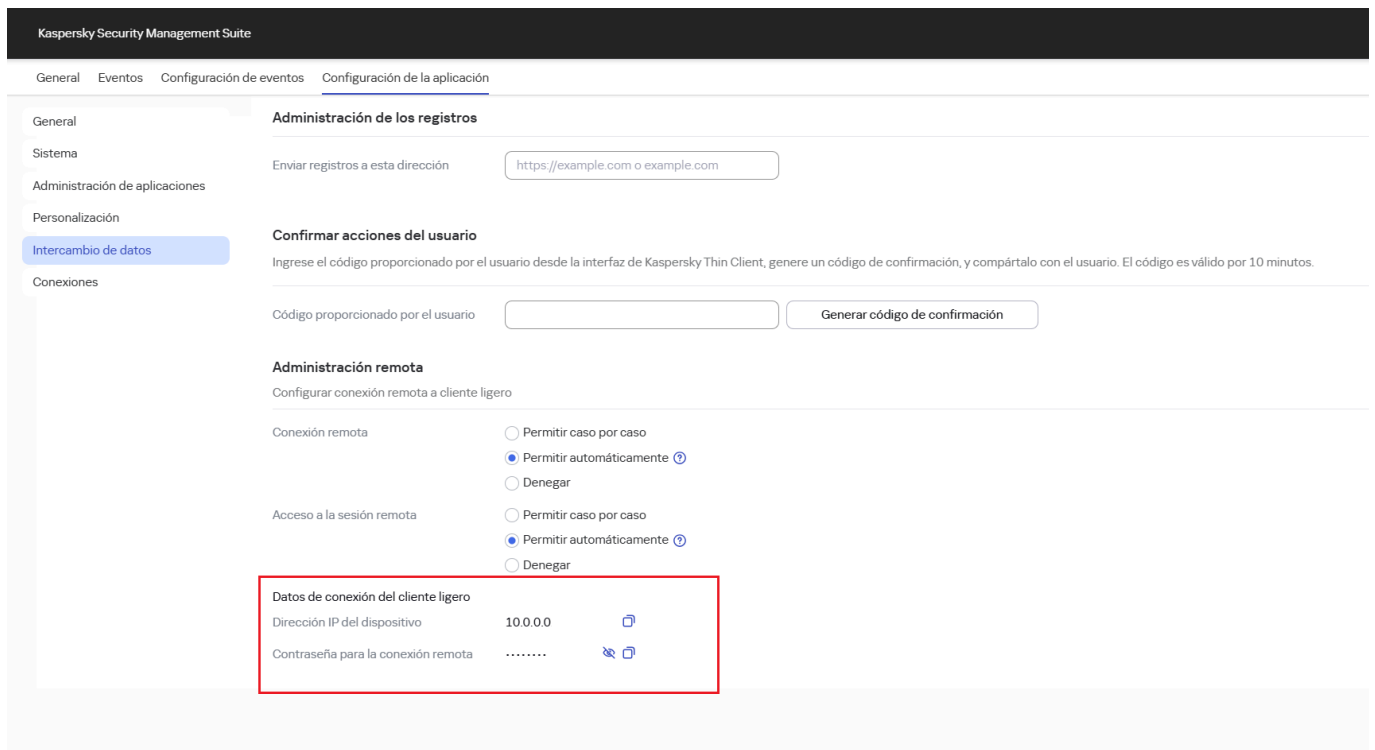
La dirección IP del cliente ligero y la contraseña de la conexión remota (en adelante también denominadas "credenciales") son necesarias para la administración remota.

Para conectarse a un cliente ligero y administrarlo a distancia:

1. Abra el cliente de RDP en el dispositivo con el que desee conectarse al cliente ligero.
2. Obtenga las credenciales de conexión remota de una de las siguientes maneras:
 - Si el cliente ligero está [conectado a Kaspersky Security Center](#), copie las credenciales de la interfaz de Web Console:
 - a. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados** si busca conectarse a un dispositivo que pertenezca a un grupo de administración; caso contrario, seleccione **Descubrimiento y despliegue** → **Dispositivos no asignados** para conectarse a un dispositivo que no forme parte de ningún grupo de administración.
 - b. En la lista que se abrirá, haga clic en el [nombre del cliente ligero](#) al que desee conectarse.
 - c. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
 - d. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
 - e. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
 - f. Vaya a la sección **Intercambio de datos**.

g. En el bloque **Datos de conexión del cliente ligero**, copie las credenciales de la cuenta de conexión remota haciendo clic en el botón  junto a ellas (consulte la imagen a continuación).

La contraseña de conexión remota disponible en Web Console se actualiza una vez al día y cada vez que se reinicia el cliente ligero.



Ventana de configuración de la administración remota de un cliente ligero en Web Console

- Si el cliente ligero no está conectado a Kaspersky Security Center, solicite la contraseña predeterminada a [Soporte técnico](#) y [obtenga la dirección IP del dispositivo en la interfaz de Kaspersky Thin Client](#).

La contraseña predeterminada está pensada para usarse en forma temporal. Úsela solo si el cliente ligero aún no está conectado a Kaspersky Security Center.

3. En el cliente RDP instalado en su dispositivo, ingrese las credenciales recibidas y comience a conectarse al cliente ligero.
4. Para conectarse al cliente ligero, dependiendo del modo de acceso específico de administración remota que se estableció en la [configuración de Kaspersky Thin Client](#) o en la configuración de administración remota de Web Console [para el dispositivo](#) o su [grupo de administración](#), realice una de las siguientes acciones.
 - Si el modo definido es **Permitir automáticamente**, espere a que se establezca la conexión con el cliente ligero.
El usuario tiene 30 segundos para aceptar o rechazar la solicitud. Si el usuario no actúa dentro de este plazo, la conexión se inicia de forma automática.
 - Si el modo definido es **Permitir caso por caso**, espere a [que el usuario acepte la solicitud de administración remota en la interfaz de Kaspersky Thin Client](#).

Si se conectó correctamente al cliente ligero, se mostrará la ventana de acceso a la pantalla del entorno remoto.

5. Para obtener acceso a la pantalla del entorno remoto, dependiendo del modo de acceso específico de administración remota que se estableció en la [configuración de Kaspersky Thin Client](#) o en la configuración de administración remota de Web Console [para el dispositivo](#) o su [grupo de administración](#), realice una de las siguientes acciones:

- Si el modo definido es **Permitir automáticamente**, espere a que se establezca la conexión con el cliente ligero.
- Si se configuró el modo **Permitir caso por caso**, espere a que el usuario acepte la solicitud de conexión en la interfaz de Kaspersky Thin Client o [termine la sesión remota](#).
- Si el modo definido es **Denegar**, espere a que el usuario ponga fin a su sesión remota.

Aparecerá la interfaz de Kaspersky Thin Client. Obtendrá acceso a la administración remota de Kaspersky Thin Client.

Para terminar la administración remota del cliente ligero en la interfaz de Kaspersky Thin Client,

en el [panel de conexión](#), haga clic en el botón . En la ventana que se abrirá, haga clic en **Terminar**.

Administrar Kaspersky Thin Client a través de Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (también llamado, en adelante, "Web Console") es una aplicación web que permite realizar, de manera centralizada, las principales tareas que se requieren para administrar y mantener el sistema de seguridad de una red empresarial. Web Console es un componente de Kaspersky Security Center que proporciona una interfaz de usuario. Para obtener información detallada sobre Kaspersky Security Center Web Console, consulte la [guía de la ayuda en línea de Kaspersky Security Center](#).

Kaspersky Thin Client 2.3 es compatible con Kaspersky Security Center Linux versión 15.3 y Kaspersky Security Center Web Console versión 15.3.

Acerca del complemento web de Kaspersky Security Management Suite

El *complemento web Kaspersky Security Management Suite* (en adelante también denominado "el complemento web") es un componente especializado que permite administrar el funcionamiento de Kaspersky Thin Client a través de Kaspersky Security Center Web Console.

El complemento web permite realizar las siguientes operaciones de manera centralizada:

- Administrar la configuración de Kaspersky Thin Client [para uno](#) o [más clientes ligeros](#) en un [grupo de administración](#).
- [Configurar la recepción de eventos de Kaspersky Thin Client y consultarlos.](#)
- [Administrar los certificados de seguridad de Kaspersky Thin Client.](#)

Para permitir la interacción entre Kaspersky Thin Client y Kaspersky Security Center, asegúrese de hacer lo siguiente:

- [Especifique los ajustes de conexión de Kaspersky Security Center](#) al configurar Kaspersky Thin Client.
- [Instale el complemento web de Kaspersky Security Management Suite](#) en Kaspersky Security Center.

Para garantizar el funcionamiento estable de las funciones del sistema y el acceso a todas sus capacidades, las versiones principales del complemento web de Kaspersky Security Management Suite y Kaspersky Thin Client deben coincidir.

Instalar el complemento web de Kaspersky Security Management Suite

Kaspersky Security Management Suite, Kaspersky Security Center y Kaspersky Security Center Web Console no forman parte del kit de distribución de Kaspersky Thin Client. Deben instalarse en forma independiente.

Puede ver la lista de complementos web instalados a través de la interfaz de Web Console (**Configuración de la consola** → **Complementos web**).

La funcionalidad del complemento web está disponible para cualquier administrador que pueda acceder a Web Console a través de un navegador. Si es necesario, puede [configurar un control de acceso para la funcionalidad de Kaspersky Security Management Suite](#).

Si piensa conectar el cliente ligero a Kaspersky Security Center a través del puerto predeterminado, asegúrese de que el puerto 13292 esté disponible en el Servidor de administración de Kaspersky Security Center. Si desea usar un puerto que no sea el 13292, configure los permisos correspondientes. Para obtener más información sobre cómo habilitar un puerto en el servidor de administración de Kaspersky Security Center, consulte la [Ayuda en línea de Kaspersky Security Center](#).

Para garantizar el funcionamiento estable de las funciones del sistema y el acceso a todas sus capacidades, las versiones principales del complemento web de Kaspersky Security Management Suite y Kaspersky Thin Client deben coincidir.

Para instalar el complemento web en Web Console:

1. En el [kit de distribución de Kaspersky Thin Client](#), busque y abra el archivo de almacenamiento pertinente que contenga las imágenes de instalación del complemento web y los archivos de firma.

Se muestra el contrato de licencia de usuario final.

2. Lea el contrato de licencia de usuario final y, si está de acuerdo con sus términos, acéptelo.

El archivo con las imágenes de instalación del complemento web y los archivos de firma se descomprimirá automáticamente luego de que acepte el contrato.

3. En la interfaz de Web Console, dentro del menú, seleccione **Configuración de la consola** → **Complementos web**.

Aparece una lista con los complementos de administración disponibles en Web Console.

4. Haga clic en el botón **Agregar desde archivo**.

5. En el panel que se abre, agregue los siguientes archivos, que se habrán extraído del archivo con las imágenes de instalación del complemento web y los archivos de firma:

- El archivo ZIP que contiene el paquete de distribución del complemento (`plugin.zip`). Para agregar este archivo, haga clic en **Cargar archivo ZIP**.
- El archivo que contiene la firma (`signature.txt`). Para agregar este archivo, haga clic en **Cargar firma**.

6. Haga clic en el botón **Agregar**.

7. Cuando finalice la instalación del complemento web, haga clic en **Aceptar**.

El complemento web Kaspersky Security Management Suite se cargará con la configuración predeterminada y aparecerá en la lista de complementos de administración de Web Console.

Actualizar el complemento web Kaspersky Security Management Suite

Para actualizar Kaspersky Security Management Suite, debe obtener de Kaspersky un archivo de almacenamiento que contenga el paquete de instalación del complemento web y la firma digital de dicho archivo.

Para actualizar el complemento web en Web Console:

1. Abra el archivo obtenido de Kaspersky con las imágenes de instalación del complemento web y los archivos de firma.

Se muestra el contrato de licencia de usuario final.

2. Lea el contrato de licencia de usuario final y, si está de acuerdo con sus términos, acéptelo.

El archivo con las imágenes de instalación del complemento web y los archivos de firma se descomprimirá automáticamente luego de que acepte el contrato.

3. En la interfaz de Web Console, dentro del menú, seleccione **Configuración de la consola** → **Complementos web**.

4. En la lista que aparece con los complementos de Web Console, busque "Kaspersky Security Management Suite" y haga clic en ese elemento.

5. En la ventana que se abre, haga clic en el botón **Actualizar desde archivo**.

6. En el panel que se abre, agregue los siguientes archivos, que se habrán extraído del archivo con las imágenes de instalación del complemento web y los archivos de firma:

- El archivo ZIP que contiene el paquete de distribución del complemento (`plugin.zip`). Para agregar este archivo, haga clic en **Cargar archivo ZIP**.
- El archivo que contiene la firma (`signature.txt`). Para agregar este archivo, haga clic en **Cargar firma**.

7. Haga clic en **Actualizar**.

8. Cuando se complete la actualización y vea la confirmación de que la instalación se realizó en forma correcta, haga clic en **Aceptar**.

El complemento web Kaspersky Security Management Suite quedará actualizado. Encontrará información sobre la versión del complemento y la hora de actualización en la tabla de complementos de Web Console.

Eliminar el complemento web Kaspersky Security Management Suite

Si lo desea, puede eliminar el complemento web Kaspersky Security Management Suite de Web Console. Si elimina este complemento web, no podrá administrar Kaspersky Thin Client mediante la interfaz de Web Console.

Antes de eliminar el complemento web, elimine de los [grupos de administración](#) los dispositivos administrados.

Para eliminar el complemento web Kaspersky Security Management Suite de Web Console:

1. En la interfaz de Web Console, dentro del menú, seleccione **Configuración de la consola** → **Complementos web**.
Aparece una lista con los complementos de administración disponibles en Web Console.
2. En la lista de complementos, marque la casilla ubicada junto al complemento web de Kaspersky Security Management Suite.
3. Haga clic en el botón **Eliminar**.
4. En la ventana que se abre, en la que se le pide confirmar la eliminación, realice una de las siguientes acciones:
 - Si desea guardar una copia de seguridad del complemento, haga clic en **Aceptar**.
Se creará una copia de seguridad del complemento. El complemento web Kaspersky Security Management Suite se eliminará de Web Console.
 - Si no desea guardar una copia de seguridad del complemento, haga clic en el botón **Omitir copia de seguridad**.
El complemento web Kaspersky Security Management Suite se eliminará de Web Console.
5. En la ventana que se abre, que contiene información sobre la eliminación del complemento, haga clic en **Aceptar**.

Restringir el acceso a las funciones del complemento web de Kaspersky Security Management Suite

Si un usuario de Kaspersky Security Center no tiene asignados [los derechos necesarios para acceder a las funciones de la aplicación](#) o no tiene asignado [el rol estándar de Kaspersky Security Center](#), no podrá trabajar con Kaspersky Security Center Web Console.

Puede configurar los derechos de usuario de Kaspersky Security Center para acceder a las funciones de la aplicación de las siguientes maneras:

- Puede configurar los derechos de cada usuario o grupo de usuarios por separado.
- Puede crear roles de Kaspersky Security Center estándares, con un conjunto de derechos predefinidos, y, luego, puede asignar esos roles a los usuarios basándose en las responsabilidades que le correspondan a cada persona.

Un *rol* es un conjunto de derechos preconfigurado que regula el acceso a las funciones de Kaspersky Security Management Suite y que puede asignarse a los usuarios. Recomendamos configurar los derechos de acceso de los roles basándose en las tareas y obligaciones típicas de los usuarios. Cuando se le asigna un rol a un usuario, se le brinda acceso a las funciones que requiere para cumplir con sus obligaciones.

Para obtener más información sobre cómo configurar el acceso basado en roles, consulte la [Ayuda en línea de Kaspersky Security Center](#).

Además de los roles estándar de Kaspersky Security Center, puede asignarles a los usuarios los siguientes roles estándar para administrar las funciones de Kaspersky Thin Client:

- *Oficial de seguridad*. Solo se permite la [administración de certificados](#) para este rol. Puede asignar este rol al empleado responsable de la seguridad de la información en la empresa.
- *Administrador*. Este rol tiene acceso a todas las funciones de administración de Kaspersky Thin Client a través de Web Console, excepto la administración de certificados.
- *Administrador avanzado*. Este rol tiene acceso a todas las funciones de administración de Kaspersky Thin Client a través de Web Console. Puede asignar este rol al empleado que sea responsable de mantener y administrar los sistemas de la información en la empresa y que esté a cargo de la seguridad de la información en la empresa.

La siguiente tabla enumera las funciones de administración de Kaspersky Thin Client que están disponibles para el usuario según el rol que le asignaron. Los ajustes de Kaspersky Thin Client correspondientes a las funciones marcadas con el ícono ✓ pueden modificarse a través de Web Console. Todos los roles pueden ver los ajustes de Kaspersky Thin Client correspondientes a todas las funciones en Web Console.

Funciones de administración de Kaspersky Thin Client disponibles en Web Console según el rol del usuario

Función	Oficial de seguridad	Administrador	Administrador avanzado
Administrar los certificados en una directiva de Kaspersky Security Management Suite	✓	–	✓
Establecer la configuración para conectarse a un entorno remoto en una directiva de Kaspersky Security Management Suite	–	✓	✓
Configurar los ajustes generales en una directiva de Kaspersky Security Management Suite	–	✓	✓
Administrar los ajustes del sistema en una directiva de Kaspersky Security Management Suite	–	✓	✓
Administrar los datos de Kaspersky Thin Client en una directiva de Kaspersky Security Management Suite	–	✓	✓
Administrar las aplicaciones de Kaspersky Thin Client en una directiva de Kaspersky Security Management Suite	–	✓	✓
Establecer la configuración de personalización en una directiva de Kaspersky Security Management Suite	–	✓	✓

Iniciar y cerrar sesión en Web Console

Para iniciar sesión en Web Console, necesitará la dirección web y el número de puerto del Servidor de administración de Kaspersky Security Center especificados durante la instalación (el puerto 8080 se usa de manera predeterminada). Asimismo, habilite JavaScript en el navegador. Para conocer los requisitos con los que debe cumplir el navegador utilizado para Kaspersky Security Center Web Console, consulte la sección [Requisitos de hardware y software](#) en la Ayuda en línea de Kaspersky Security Center.

Para iniciar sesión en Web Console:

1. En el navegador, vaya a `https://<dirección del Servidor de administración>:<número de puerto>`.

Se abre la página de inicio de sesión.

2. Inicie sesión con el nombre de usuario y la contraseña del dominio.

Si el Servidor de administración no responde o si las credenciales ingresadas no son correctas, se mostrará un mensaje de error.

Una vez que se inicie la sesión, aparecerá el panel en el último idioma y con el último tema utilizados. Puede navegar a través de Web Console y usarla para trabajar con Kaspersky Security Center.

Para cerrar sesión en Web Console:

1. En la esquina inferior derecha de la pantalla, haga clic en el nombre de usuario.
2. En el menú que se abre, seleccione **Salir**.

Web Console se cerrará y aparecerá la página de inicio de sesión.

Administrar directivas y grupos de administración

En Web Console, puede agregar clientes ligeros que ejecuten Kaspersky Thin Client y estén conectados a Kaspersky Security Center a un [grupo de administración](#) para [establecer la configuración del sistema](#) de forma centralizada mediante [directivas](#).

De forma predeterminada, inmediatamente después de instalar Kaspersky Security Center, ya existe un grupo en la jerarquía de grupos de administración: **Dispositivos administrados**. Cualquier grupo que usted cree será un grupo secundario de este grupo. En la directiva creada el grupo **Dispositivos administrados**, puede configurar dispositivos para todos los grupos de administración. Por ejemplo, recomendamos utilizar la directiva para tareas como [agregar certificados](#) de forma centralizada. Para obtener más información sobre la jerarquía de grupos y directivas, consulte la [Ayuda en línea de Kaspersky Security Center](#).

Esta sección proporciona instrucciones para crear grupos de administración y agregarles clientes ligeros, y sobre cómo crear y editar directivas. Para obtener más información, consulte las secciones [directiva](#) y [administración de dispositivos](#) de la Ayuda de Kaspersky Security Center.

Crear un grupo de administración

En Web Console, puede crear [grupos de administración](#) y agregar clientes ligeros que ejecuten Kaspersky Thin Client y estén conectados a Kaspersky Security Center a estos grupos para [configurar los ajustes del dispositivo](#) utilizando [directivas](#) de manera centralizada.

Para crear un grupo de administración:

1. En la ventana principal de la Web Console, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. Marque la casilla junto al grupo de administración al que debe pertenecer el nuevo grupo.
Si aún no ha creado ningún grupo de administración, seleccione el grupo **Dispositivos administrados**.
3. Haga clic en el botón **Agregar**.
4. En el panel que se abre, escriba el nombre de un nuevo grupo de administración y haga clic en **Agregar**.

El nombre de un grupo de administración debe ser único dentro de su jerarquía.

El nuevo grupo aparecerá en la lista de grupos de administración.

Agregar clientes ligeros al grupo de administración

Puede agregar clientes ligeros que ejecuten Kaspersky Thin Client al [grupo de administración que creó](#) o al grupo **de dispositivos administrados**.

Para agregar dispositivos al grupo de administración:

1. En la ventana principal de Web Console, seleccione **Descubrimiento y despliegue** → **Dispositivos no asignados**.
Se mostrará una lista de todos los dispositivos que están conectados a Kaspersky Security Center, pero no han sido agregados a ningún grupo de administración.
2. Seleccione las casillas de verificación junto a los dispositivos que desea agregar al grupo.
3. Haga clic en el botón **Mover**.
4. En el panel que aparece, seleccione el grupo de administración.
5. Haga clic en el botón **Mover**.

Los dispositivos se agregarán al grupo de administración seleccionado.

También puede automatizar la transferencia de clientes ligeros a grupos de administración. Para obtener más información, consulte la [Ayuda en línea de Kaspersky Security Center](#).

Crear una directiva

Para configurar el Kaspersky Thin Client que se instaló en los clientes ligeros de un [grupo de administración](#), cree una [directiva](#) para ese grupo en Web Console.

De forma predeterminada, inmediatamente después de instalar Kaspersky Security Center, ya existe un grupo en la jerarquía de grupos de administración: **Dispositivos administrados**. Cualquier grupo que usted cree será un grupo secundario de este grupo. En la directiva creada el grupo **Dispositivos administrados**, puede configurar dispositivos para todos los grupos de administración. Por ejemplo, recomendamos utilizar la directiva para tareas como [agregar certificados](#) de forma centralizada. Para obtener más información sobre la jerarquía de grupos y directivas, consulte la [Ayuda en línea de Kaspersky Security Center](#).

Para crear una directiva:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Seleccione el grupo de administración requerido. Para ello, haga clic en la ruta actual en la parte superior de la ventana y, en el panel que se abre, haga clic en el grupo de administración requerido.
3. Haga clic en el botón **Agregar**.
4. En la lista de aplicaciones que se muestra en la ventana que se abre, seleccione el complemento web de administración de Kaspersky Thin Client y haga clic en **Siguiente**.
5. En la ventana de configuración de la nueva directiva, en la pestaña **General**, defina los siguientes ajustes:
 - En el campo **Nombre**, ingrese el nombre de la directiva.
 - En el bloque **Estado de la directiva**, seleccione uno de los siguientes estados:
 - **Activa**
La directiva que está aplicada actualmente a los dispositivos del grupo de administración. Si esta opción está seleccionada, la siguiente vez que sincronice Kaspersky Thin Client y Kaspersky Security Center, esta directiva se activará. Cada grupo de administración solo puede tener una directiva activa. Este es el estado preseleccionado.
 - **Inactiva**
La directiva que no está aplicada actualmente a los dispositivos del grupo de administración. Si esta opción está seleccionada, la directiva se torna inactiva pero permanece en la lista de directivas. Una política inactiva se puede activar más adelante.
 - **Fuera de la oficina**
La directiva se activa cuando el dispositivo abandona el perímetro de la red de la organización.
 - Activar o desactivar los botones en el bloque **Herencia de configuración**:
 - **Heredar configuración de la directiva primaria**
Si el conmutador está habilitado, las configuraciones de directiva se heredan de la directiva del grupo de nivel superior y no se pueden modificar.

De forma predeterminada, la opción está habilitada.

- **Forzar la herencia de configuraciones en las directivas secundarias**

Los ajustes de la directiva se propagarán a las directivas de los grupos de administración anidados (directivas secundarias) y, en el bloque **Herencia de configuraciones**, en la sección **General** de cada ventana de propiedades de directiva secundaria, se habilitará automáticamente la opción **Heredar configuración de la directiva primaria**.

Cuando esta configuración está habilitada, las configuraciones de la directiva secundaria no se pueden modificar.

De forma predeterminada, esta opción está deshabilitada.

Para obtener más información sobre la jerarquía de grupos y directivas, consulte la [Ayuda en línea de Kaspersky Security Center](#).

6. Si desea [personalizar otros ajustes](#), seleccione la pestaña **Configuración de la aplicación** y realice los cambios necesarios.

7. Haga clic en el botón **Guardar** en la parte inferior de la página.

La directiva se crea y aparece en la lista de directivas.

Modificar una directiva

En Web Console, puede editar una [directiva existente](#).

Para modificar una directiva:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Seleccione la directiva que desee modificar.
3. En la ventana de configuración de directivas que aparece, ajuste la configuración [según sea necesario](#) en la pestaña **General**.
4. Haga clic en el botón **Guardar** ubicado en la parte inferior de la página.

Se guardarán los cambios realizados en la directiva y se los mostrará en las propiedades de la directiva, dentro de la sección **Historial de revisiones**.

Bloquear ajustes en una directiva

En cada [directiva](#), los ajustes tienen un interruptor de bloqueo con un ícono de candado. Las posiciones disponibles en el interruptor se describen en la siguiente tabla.

Posiciones del interruptor de bloqueo de los ajustes

Estado	Descripción
 Sin definir 	Los valores asignados a este ajuste no se aplican a los dispositivos regidos por la directiva. El usuario puede cambiar este ajuste en la interfaz de usuario de Kaspersky Thin Client.
 Imponer 	Los valores asignados a este ajuste se aplican a los dispositivos regidos por la directiva. El usuario no podrá cambiar esta configuración en la interfaz de Kaspersky Thin Client.

Configurar los parámetros de Kaspersky Thin Client para un dispositivo a través de Web Console

En Web Console, puede configurar los ajustes de Kaspersky Thin Client instalado en un cliente ligero. El dispositivo debe estar conectado a Kaspersky Security Center y debe [estar agregado a un grupo de administración](#).

Cambiar el id. de un cliente ligero a través de Web Console: un dispositivo

En Kaspersky Security Center Web Console, puede cambiar el identificador de un cliente ligero [agregado a un grupo de administración](#), si ya existe un dispositivo con el mismo nombre en este grupo de administración.

Puede [usar directivas](#) para configurar los nombres de dispositivos en un grupo de administración.

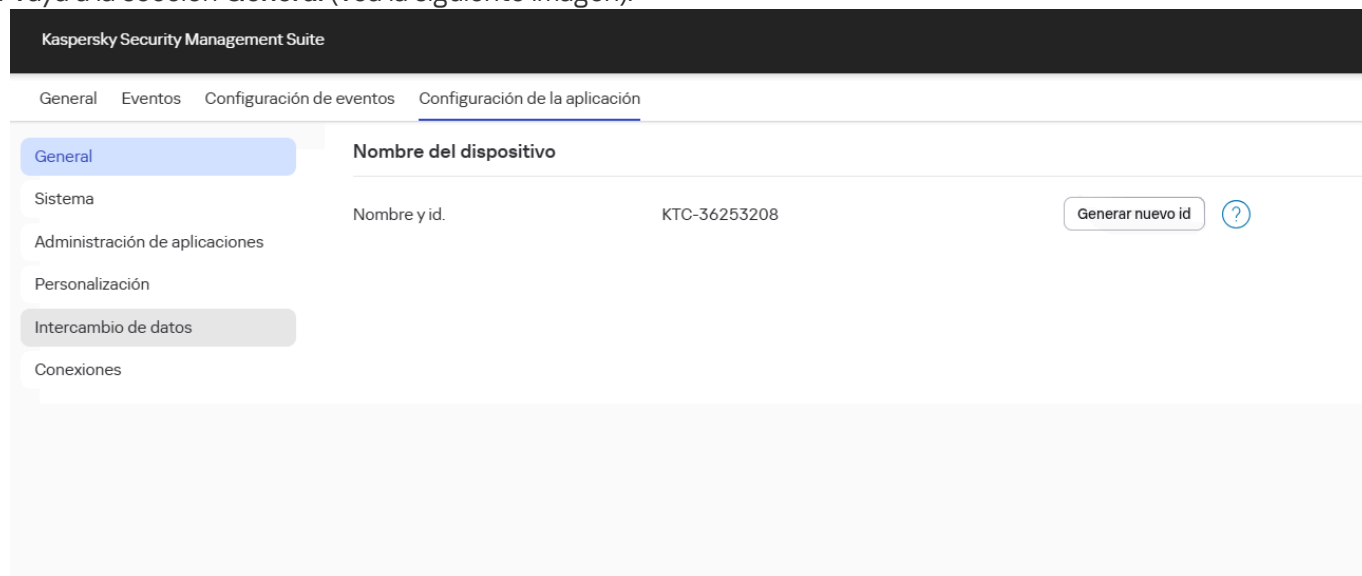
Para cambiar el id. De un cliente ligero a través de Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agreguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.

6. Vaya a la sección **General** (vea la siguiente imagen).



Cambio del id. de un cliente ligero mediante la Consola web

7. En el grupo **Nombre del dispositivo**, haga clic en **Generar nuevo id**.

Esto da inicio al proceso de creación de un nuevo id. Se actualizará en la interfaz de Web Console después de que el cliente ligero se sincronice con Kaspersky Security Center.

8. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardan y se aplican al Kaspersky Thin Client instalado en el cliente ligero después de sincronizar Kaspersky Thin Client con Kaspersky Security Center.

Configurar la conexión a un entorno remoto usando la aplicación RDP a través de Web Console: un dispositivo

En Web Console, puede configurar los ajustes para [conectarse a un entorno remoto usando la aplicación RDP](#).

Para configurar los ajustes para conectarse a un entorno remoto usando la aplicación RDP:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agreguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.

6. Seleccione **Conexiones** → **RDP**.

Se abre una ventana para configurar los ajustes que se usarán al conectarse al entorno remoto (vea la siguiente imagen).

Kaspersky Security Management Suite

General Eventos Configuración de eventos Configuración de la aplicación

General Sistema Administración de aplicaciones Personalización Intercambio de datos **Conexiones**

RDP Basis.WorkPlace Web Access

Ajustes del servidor RDP

Introduzca o cargue los ajustes de conexión al servidor

Nombre de usuario

Dirección IP o nombre del servidor 192.168.2.0 o example.com

Avanzado

Id. de colección del Agente de conexión a Escritorio remoto Por ejemplo, tsv://MS Terminal Services Plu...

Alias de la aplicación (cuando se conecta de forma remota, solo se abre la aplicación con este alias) Introduzca un alias

Cargar archivo de configuración

Conexión automática

☐ Conectarse automáticamente

La contraseña ingresada para la última conexión correcta se guardará y se usará. Se recomienda activar esta opción solo si no hay personas no autorizadas que tengan acceso al cliente ligero.

Recuperación de la conexión

☐ Conectar de nuevo si se pierde la conexión

Ventana para configurar la conexión a un entorno remoto en la aplicación RDP mediante Web Console

- En el campo de **dirección IP o nombre del servidor**, ingrese la dirección IP o el nombre del servidor del Agente de conexión a Escritorio remoto de Microsoft.
- En el campo **Nombre de usuario**, ingrese el nombre de la cuenta de usuario con la que se establecerá la conexión.
- Si desea usar el Agente de conexión a Escritorio remoto de Microsoft para conectarse a un escritorio remoto, en el campo **Id. de colección del Agente de conexión a Escritorio remoto**, ingrese el id. de la colección en formato `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` hace referencia al identificador específico de la colección).

Si desea iniciar una aplicación virtual, ingrese el alias de la aplicación en el campo **Alias de la aplicación**.

Si tiene un archivo de configuración que contiene los ajustes para conectarse al Agente de conexión al Escritorio remoto de Microsoft y, si es necesario, el nombre de la aplicación para abrir, haga clic en el botón **Cargar archivo de configuración** y cargue el archivo. En ese caso, no necesitará completar el campo **Id. de colección del Agente de conexión a Escritorio remoto** y **Alias de la aplicación**.

- Si desea que la conexión se restablezca automáticamente ante una desconexión inesperada, marque la casilla **Conectar de nuevo si se pierde la conexión**.
- En el bloque de ajustes **Redirección de dispositivos**, seleccione los dispositivos que se redirigirán al entorno remoto: **Tarjetas inteligentes, Unidades de memoria USB, Impresoras y otros dispositivos, Micrófono, Dispositivos de reproducción de audio, Cámara web (video), Escáner**.
El volumen del audio y otros ajustes se controlan desde el entorno remoto.

Para redireccionar dispositivos USB a un escritorio remoto que ejecute el sistema operativo Windows 10, es necesario habilitar los Servicios de Escritorio remoto de Microsoft y permitir la redirección de dispositivos Plug and Play en la configuración de los Servicios de Escritorio remoto. En el caso de Microsoft Windows Server 2016 o 2019, también se deben permitir las conexiones remotas a través de los Servicios de Escritorio remoto y se debe permitir la configuración de reglas de control remoto en los Servicios de Escritorio remoto.

12. En el bloque **Calidad de la imagen**, seleccione las casillas junto a la configuración gráfica del escritorio remoto que desea usar: **Suavizar fuentes**, **Animación de menús**, **Fondo de escritorio**, **Mostrar el contenido de las ventanas al arrastrarlas**, **Tema mejorado**.

Si habilita las opciones gráficas del escritorio remoto, podría verse afectada la velocidad de las operaciones de Kaspersky Thin Client.

13. Si su estación de trabajo tiene dos monitores y desea que la imagen del escritorio remoto se muestre en ambos, marque la casilla **Usar dos monitores** en el bloque **Administración de monitores**.
14. Para mejorar el rendimiento cuando se conecte a aplicaciones o escritorios remotos, en el bloque **Rendimiento**, marque **Mejorar el rendimiento gráfico**.

15. Para conectarse automáticamente a un escritorio remoto o una aplicación virtual cuando se inicie la aplicación RDP, en el bloque **Conexión automática**, seleccione la casilla **Conectarse automáticamente**.

Para activar esta función, el usuario debe conectarse manualmente y desconectarse del entorno remoto una vez. Cuando lo hace, los siguientes datos para conectarse al servidor RDP se guardan en el almacenamiento del cliente ligero: nombre de usuario, dirección del servidor y contraseña. La siguiente vez que inicie la aplicación RDP, estas credenciales se usarán para iniciar automáticamente una conexión con el entorno remoto. Si deshabilita la función de conexión automática, la contraseña guardada se elimina del almacenamiento del dispositivo.

Web Console no le permite establecer una contraseña para conectarse a un entorno remoto.

Para conectarse automáticamente al entorno remoto en la aplicación RDP inmediatamente después de iniciar Kaspersky Thin Client, [configure el inicio automático de la aplicación](#).

16. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardan y se aplican al Kaspersky Thin Client instalado en el cliente ligero después de sincronizar Kaspersky Thin Client con Kaspersky Security Center.

Configurar la conexión a un entorno remoto usando la aplicación Basis.WorkPlace a través de Web Console: un dispositivo

En la aplicación Web Console, puede configurar los ajustes que se usarán para conectarse a un entorno remoto implementado en una infraestructura de Basis.WorkPlace.

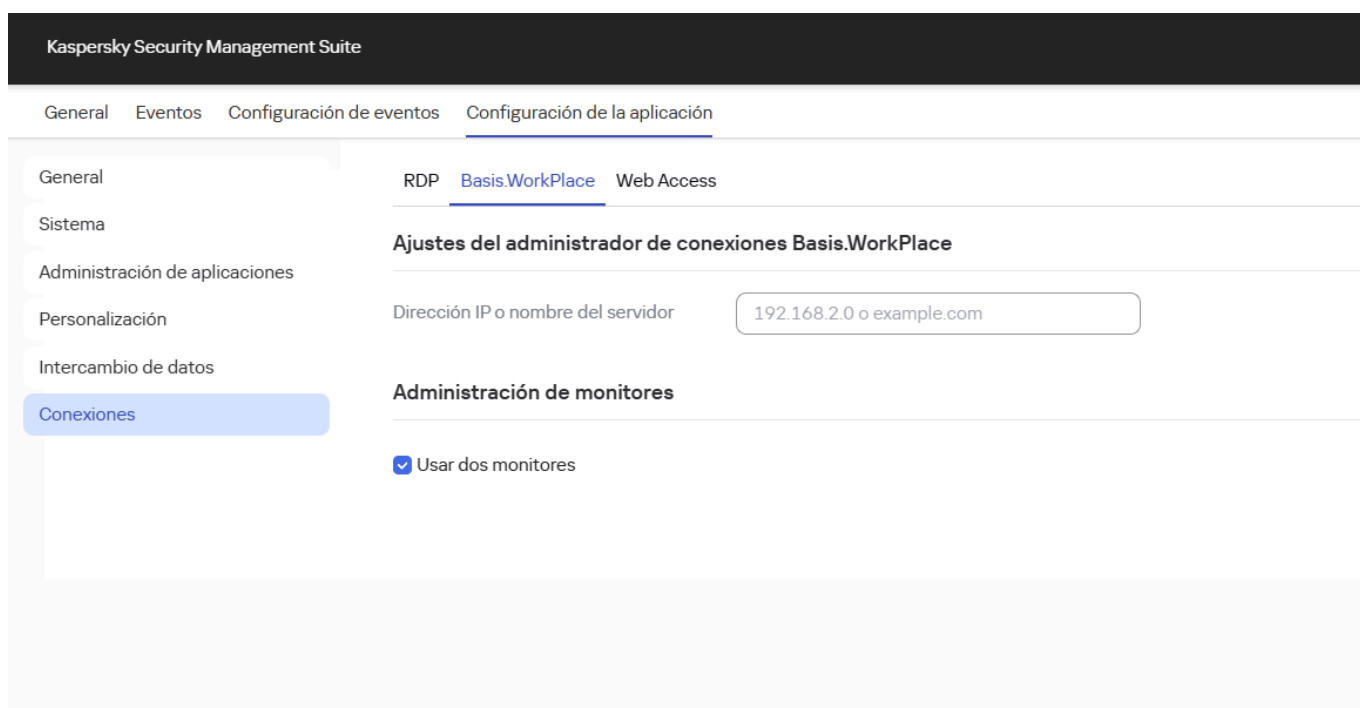
Los usuarios no pueden iniciar un cambio de contraseña en Kaspersky Thin Client.

Para configurar los ajustes para conectarse a un entorno remoto desplegado en la infraestructura de Basis.WorkPlace:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agréguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Seleccione **Conexiones** → **Basis.WorkPlace**.
Se abre una ventana para configurar los ajustes que se usarán al conectarse al entorno remoto (vea la siguiente imagen).



Ventana para configurar los ajustes de conexión a un entorno remoto implementado en la aplicación Basis.WorkPlace mediante Web Console

7. En **Dirección IP o nombre del servidor**, ingrese la dirección IP o el nombre del servidor al que desee conectarse.
8. Si su estación de trabajo tiene dos monitores y desea que la imagen del escritorio remoto se muestre en ambos, marque la casilla **Usar dos monitores** en el bloque **Administración de monitores**.
9. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardan y se aplican al Kaspersky Thin Client instalado en el cliente ligero después de sincronizar Kaspersky Thin Client con Kaspersky Security Center.

Configurar una conexión a un entorno remoto en la aplicación Web Access a través de Web Console: un dispositivo

En Web Console, puede configurar los ajustes de [conexión a un entorno remoto en la aplicación Web Access](#).

En la aplicación Web Access, puede conectarse a un entorno remoto desplegado en infraestructuras Citrix Workspace. Web Access admite HTML5 y proporciona una conexión HTTPS segura al conectarse.

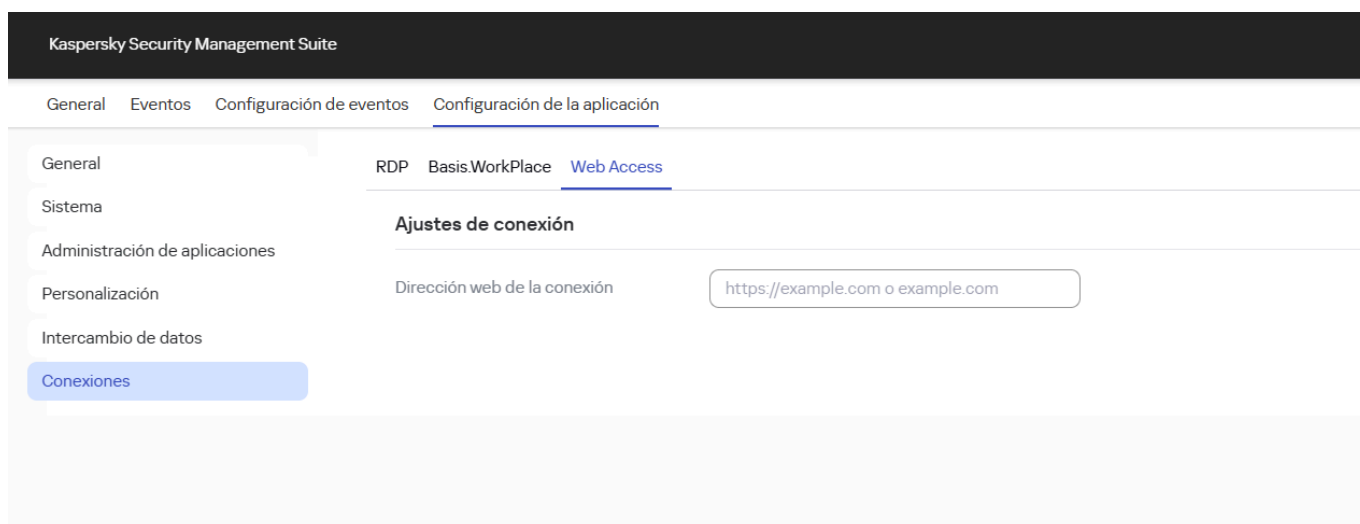
Para configurar los ajustes para conectarse a un entorno remoto usando la aplicación Web Access:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agreguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Seleccione **Conexiones** → **Web Access**.

Se abre una ventana para configurar los ajustes que se usarán al conectarse al entorno remoto (vea la siguiente imagen).



Ventana de configuración para conectarse a un entorno remoto en Web Access a través de Web Console

7. En el campo **Dirección web de la conexión**, ingrese la dirección web del servidor que se usará para conectarse al [entorno remoto correspondiente](#).

8. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardan y se aplican al Kaspersky Thin Client instalado en el cliente ligero después de sincronizar Kaspersky Thin Client con Kaspersky Security Center.

Configuración de monitores y pantallas a través de Web Console: un dispositivo

En Web Console, puede configurar los monitores conectados a un cliente ligero incluido en un [grupo de administración](#) y sus ajustes de pantalla.

Kaspersky Thin Client permite conectar dos monitores. El sistema considera que uno de los monitores es el principal y el otro, secundario. Durante una [sesión remota](#), el panel de conexión se muestra en la pantalla del monitor principal. La pantalla del monitor secundario amplía o duplica la imagen del monitor principal. En Web Console, puede seleccionar qué monitor debe considerarse el monitor principal (en adelante, también "cambiar el diseño del monitor").

En la interfaz de Web Console, los monitores están numerados. El sistema asigna números a los monitores según el puerto al que estén conectados: el monitor 1 es el conectado al puerto más cercano a la fuente de alimentación y el monitor 2 es el siguiente. Consulte la documentación del fabricante del dispositivo para conocer la ubicación de los puertos en [los modelos de cliente ligero compatibles](#).

Web Console no muestra información sobre cuántos monitores están conectados a un cliente ligero específico.

Si desea que la pantalla de la sesión remota se muestre en ambos monitores, habilítelos en la configuración de conexión del entorno de conexión remota en las aplicaciones [RDP](#) o [Basis.WorkPlace](#).

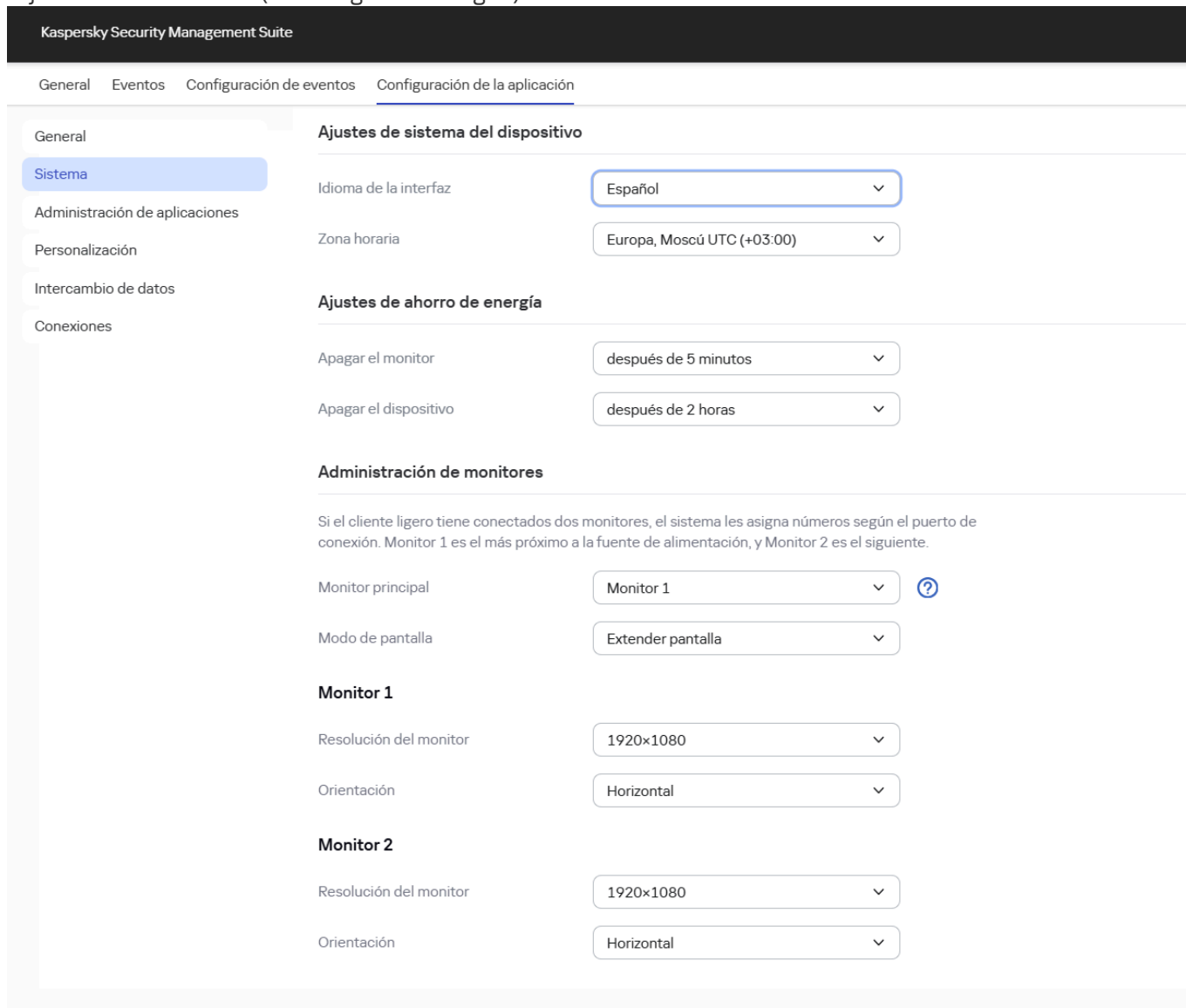
Para configurar monitores y pantallas mediante Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agréguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.

6. Elija la sección **Sistema** (vea la siguiente imagen).



Ventana para configurar los monitores y las pantallas mediante Web Console

7. En el grupo de **Administración de monitores**, configure los ajustes necesarios:

- En la lista desplegable **Monitor principal**, seleccione qué monitor debe considerarse principal.

Si solo hay un monitor conectado al cliente ligero, se le aplicarán los ajuste del monitor establecido como principal en Web Console.

- En la lista desplegable **Modo de pantalla**, seleccione la opción de visualización de imagen:
 - **Extender pantalla**: la imagen se extiende a lo largo de dos monitores.
 - **Duplicar pantalla**: la imagen de la pantalla del monitor principal se duplica en el secundario.
- En la lista desplegable **Resolución del monitor**, seleccione la resolución que desea para la pantalla seleccionada.

Las resoluciones admitidas se enumeran [en la sección de requisitos de hardware y software](#).

Si el valor **Máxima posible** está seleccionado, se establece el valor más alto del parámetro admitido por el monitor y por Kaspersky Thin Client.

- En la lista desplegable **Orientación**, seleccione la posición de la pantalla:
 - **Horizontal**: la posición estándar de la pantalla.
 - **Horizontal invertido**: la pantalla gira 180°.
 - **Vertical**: la pantalla gira 90°.
 - **Vertical invertido**: la pantalla gira 270°.

8. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardan y se aplican al Kaspersky Thin Client instalado en el cliente ligero después de sincronizar Kaspersky Thin Client con Kaspersky Security Center.

Configurar los ajustes de sistema de Kaspersky Thin Client a través de Web Console: un dispositivo

En Web Console, puede configurar el idioma de la interfaz y la zona horaria de Kaspersky Thin Client. También puede configurar la hora de apagado para el cliente ligero y los monitores que tenga conectados.

La interfaz de Kaspersky Thin Client 2.3 está disponible en los siguientes idiomas: ruso, inglés (EE. UU.), español (México) y portugués (Brasil).

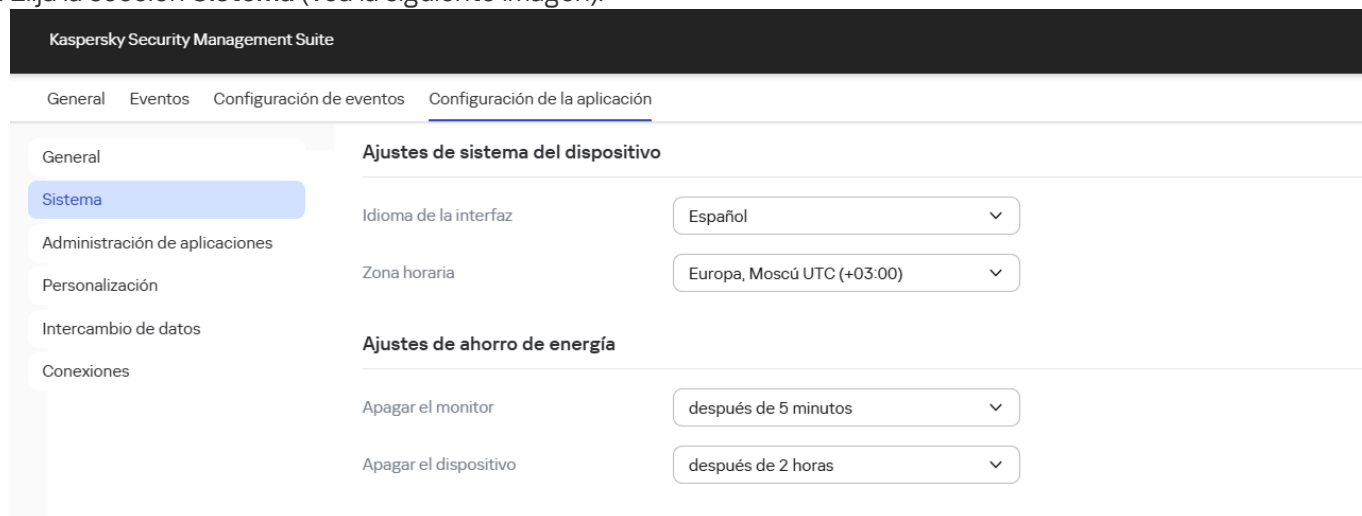
Para configurar los ajustes del sistema de Kaspersky Thin Client mediante Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agreguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.

6. Elija la sección **Sistema** (vea la siguiente imagen).



Ventana para configurar los ajustes de sistema de Kaspersky Thin Client mediante Web Console

7. En el bloque **Ajustes de sistema del dispositivo**, en las listas desplegables **Idioma de la interfaz** y **Zona horaria**, seleccione los valores pertinentes.

8. En el bloque **Ajustes de ahorro de energía**, configure los siguientes ajustes:

- En la lista desplegable **Apagar el monitor**, seleccione el período de inactividad del sistema después del cual se apagará el monitor.
- En la lista desplegable **Apagar el dispositivo**, seleccione el período de inactividad del sistema después del cual se apagará el cliente ligero.

9. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardan y se aplican al Kaspersky Thin Client instalado en el cliente ligero después de sincronizar Kaspersky Thin Client con Kaspersky Security Center.

Configurar el envío de los registros de Kaspersky Thin Client a un servidor de registros: un dispositivo

En Web Console, puede cambiar la dirección del [servidor de registros](#) al que se reenvían los [registros de eventos](#) y [auditoría](#) de Kaspersky Thin Client.

Para configurar el reenvío de los registros de Kaspersky Thin Client al servidor de registros a través de Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agréguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Elija la sección **Intercambio de datos** (vea la siguiente imagen).

Ventana para configurar el reenvío de los registros de Kaspersky Thin Client mediante Web Console

7. En el campo **Enviar registros a esta dirección**, ingrese la dirección del servidor de registros de destino en formato `https://<dirección del servidor>`.

Para recibir registros de eventos y registro de auditoría de Kaspersky Thin Client, su organización debe tener implementado un servidor de registros que cumpla con los [requisitos de hardware y software](#).

8. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardan y se aplican al Kaspersky Thin Client instalado en el cliente ligero después de sincronizar Kaspersky Thin Client con Kaspersky Security Center.

Personalizar Kaspersky Thin Client: un dispositivo

En Web Console, puede cargar sus imágenes y definir las como fondo de pantalla para el escritorio o la pantalla de bloqueo de Kaspersky Thin Client. Se admiten los formatos de archivo JPEG, PNG y JPG. El tamaño máximo que puede tener cada archivo es de 15 MB. De ser necesario, puede eliminar las imágenes que haya cargado a través de Web Console.

De manera predeterminada, el escritorio y la pantalla de bloqueo de Kaspersky Thin Client tienen un fondo estándar. Si ha configurado un fondo, puede restablecer su configuración personalizada y restaurar la imagen predeterminada.

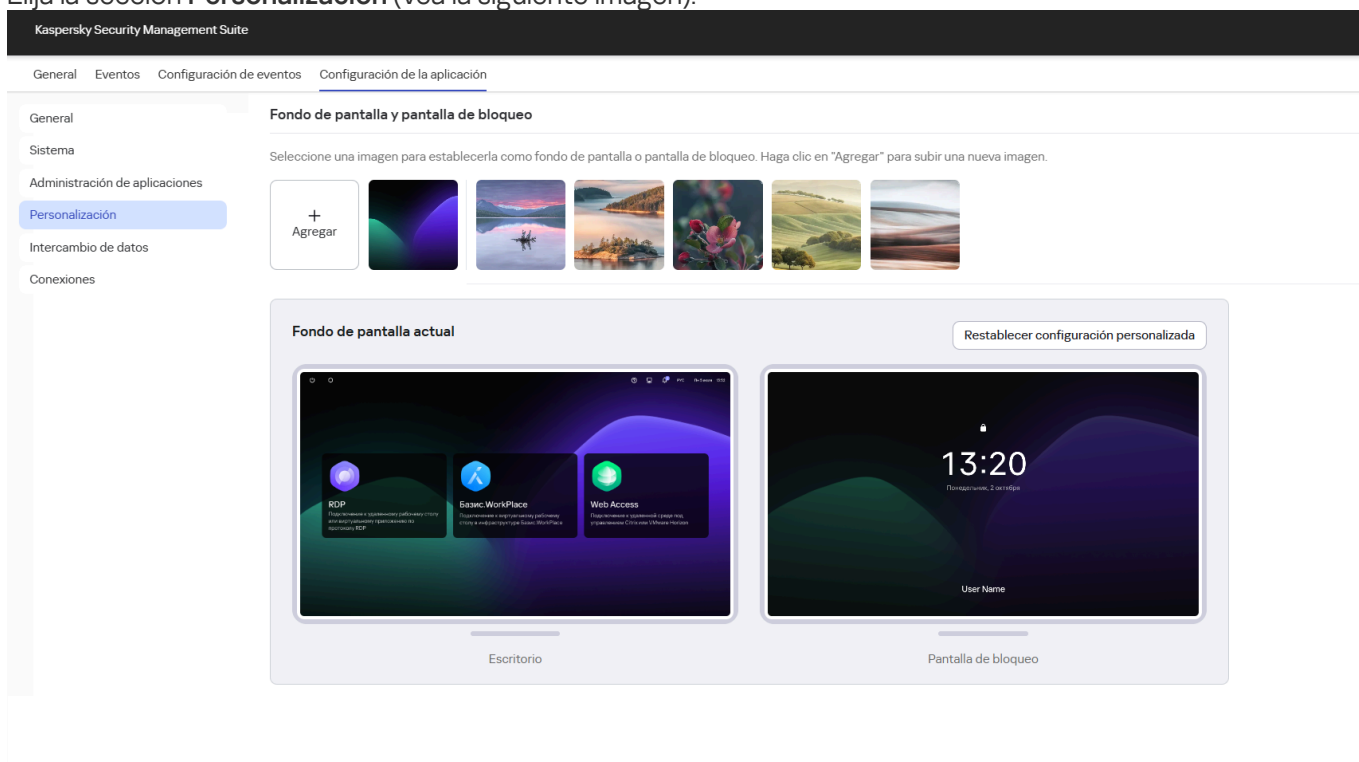
No puede cambiar el fondo en la interfaz de Kaspersky Thin Client. Puede cambiar el fondo de las pantallas solo a través de Web Console. La imagen configurada a través de Web Console también cambia al fondo estándar [si se realiza el restablecimiento a la configuración de fábrica](#).

Para cambiar el fondo del escritorio o de la pantalla de bloqueo de Kaspersky Thin Client:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agréguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Elija la sección **Personalización** (vea la siguiente imagen).



Ventana para configurar la personalización de Kaspersky Thin Client mediante Web Console.

7. Para cambiar el fondo del escritorio o de la pantalla de bloqueo, siga estos pasos:
 - a. Seleccione la imagen que desee usar de fondo.
 - Si desea cargar una nueva imagen a Web Console, haga clic en el botón **Agregar**.
En la ventana que se abre, arrastre la imagen deseada al área de carga o haga clic en **Cargar un archivo o arrástrelo y suéltelo aquí**. A continuación, en la ventana que aparezca, seleccione la imagen que desee.
 - Si desea usar una imagen que ya se haya cargado en Web Console, haga clic en la miniatura de la imagen.

Aparecerá una ventana para previsualizar dónde se ubicará la imagen seleccionada en las pantallas de Kaspersky Thin Client.

Si desea guardar la imagen en Web Console sin establecerla como fondo, vaya al paso c. de estas instrucciones.

b. Marque las casillas adyacentes a las pantallas en las que desee usar la imagen como fondo:

- **Escritorio:** la imagen se establecerá como [fondo de escritorio de Kaspersky Thin Client](#).
- **Pantalla de bloqueo:** la imagen se establecerá como [fondo de la pantalla de bloqueo](#).

c. Haga clic en **Guardar** en la ventana de previsualización.

Se mostrará la pantalla principal de la sección **Personalización**. Se cambiará el fondo de las pantallas seleccionadas.

8. Para eliminar una imagen cargada en Web Console, ubique el cursor sobre la miniatura de la imagen y haga clic en el botón  que aparecerá.

Confirme sus acciones en la ventana que aparecerá.

La imagen se eliminará de Web Console permanentemente. Si se ha establecido una imagen como fondo en alguna pantalla, se la cambiará por el fondo estándar.

9. Para restaurar el fondo estándar en todas las pantallas, haga clic en **Restablecer configuración personalizada** y confirme sus acciones en la ventana que se abrirá.

Se pondrá un fondo estándar en el escritorio y en la pantalla de bloqueo de Kaspersky Thin Client.

10. Haga clic en el botón **Guardar** en la parte inferior de la sección **Personalización**.

Los cambios se guardarán y se aplicarán al cliente ligero en el plazo de una hora después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

Configurar los ajustes para la conexión remota de un cliente ligero a través de Web Console: un dispositivo

En Web Console, puede configurar los siguientes ajustes de la conexión remota de un cliente ligero:

- **Modo de acceso a la administración remota:** determina las condiciones y el procedimiento para conectarse al cliente ligero.
- **Modo de acceso a la sesión remota** que esté activa en el cliente ligero al establecer conexión con él (en lo sucesivo, para referirse a esta sesión, también se usará el término "pantalla del entorno remoto").

Puede restringir el acceso a la pantalla del entorno remoto si el usuario del cliente ligero trabaja con datos confidenciales o privados.

Si desea configurar los ajustes para la conexión remota de un cliente ligero:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agreguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Elija la sección **Intercambio de datos** (vea la siguiente imagen).

Kaspersky Security Management Suite

General Eventos Configuración de eventos Configuración de la aplicación

General

Sistema

Administración de aplicaciones

Personalización

Intercambio de datos

Conexiones

Administración de los registros

Enviar registros a esta dirección

Confirmar acciones del usuario

Ingrese el código proporcionado por el usuario desde la interfaz de Kaspersky Thin Client, genere un código de confirmación, y compártalo con el usuario. El código es válido por 10 minutos.

Código proporcionado por el usuario

Administración remota

Configurar conexión remota a cliente ligero

Conexión remota ☒ Permitir caso por caso ☐ Permitir automáticamente ⓘ ☐ Denegar

Acceso a la sesión remota ☒ Permitir caso por caso ☐ Permitir automáticamente ⓘ ☐ Denegar

Datos de conexión del cliente ligero

Dirección IP del dispositivo 10.0.0.0

Contraseña para la conexión remota

Ventana para configurar la administración remota de clientes ligeros a través de Web Console

7. En la sección **Administración remota**, seleccione el modo de acceso a la capacidad de administración remota del cliente ligero:

- **Permitir automáticamente**

Si selecciona este modo, el administrador podrá conectarse al cliente ligero remoto después de que el usuario [acepte la solicitud de administración remota en la interfaz de Kaspersky Thin Client](#). Si el usuario rechaza la solicitud, la conexión se finalizará. Si no hay respuesta en 30 segundos, la conexión se establece automáticamente.

- **Permitir caso por caso**

En este modo, el administrador podrá conectarse de forma remota al cliente ligero solo después de que el usuario [acepte la solicitud de administración remota en la interfaz de Kaspersky Thin Client](#). Si el usuario rechaza la solicitud, la conexión se finalizará.

- **Denegar**

Si selecciona este modo, el administrador no podrá conectarse al cliente ligero remoto.

Si selecciona los modos **Permitir automáticamente** o **Permitir caso por caso**, se desbloqueará el grupo de opciones **Acceso a la sesión remota**.

8. En el grupo de opciones **Acceso a la sesión remota**, seleccione el modo de acceso a la pantalla del entorno remoto:

- **Permitir automáticamente**

Si selecciona este modo, tras conectarse al cliente ligero, el administrador podrá acceder a la pantalla del entorno remoto sin que el usuario confirme la acción.

- **Permitir caso por caso**

Si selecciona este modo, tras conectarse al cliente ligero, el administrador podrá acceder a la pantalla del entorno remoto únicamente si el usuario [acepta la solicitud de acceso en la interfaz de Kaspersky Thin Client](#).

- **Denegar**

Si selecciona este modo, el administrador no podrá administrar el cliente ligero a distancia hasta que el usuario cierre manualmente su sesión remota.

9. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardan y se aplican al Kaspersky Thin Client instalado en el cliente ligero después de sincronizar Kaspersky Thin Client con Kaspersky Security Center.

Configurar el inicio automático y la visualización de aplicaciones: un dispositivo

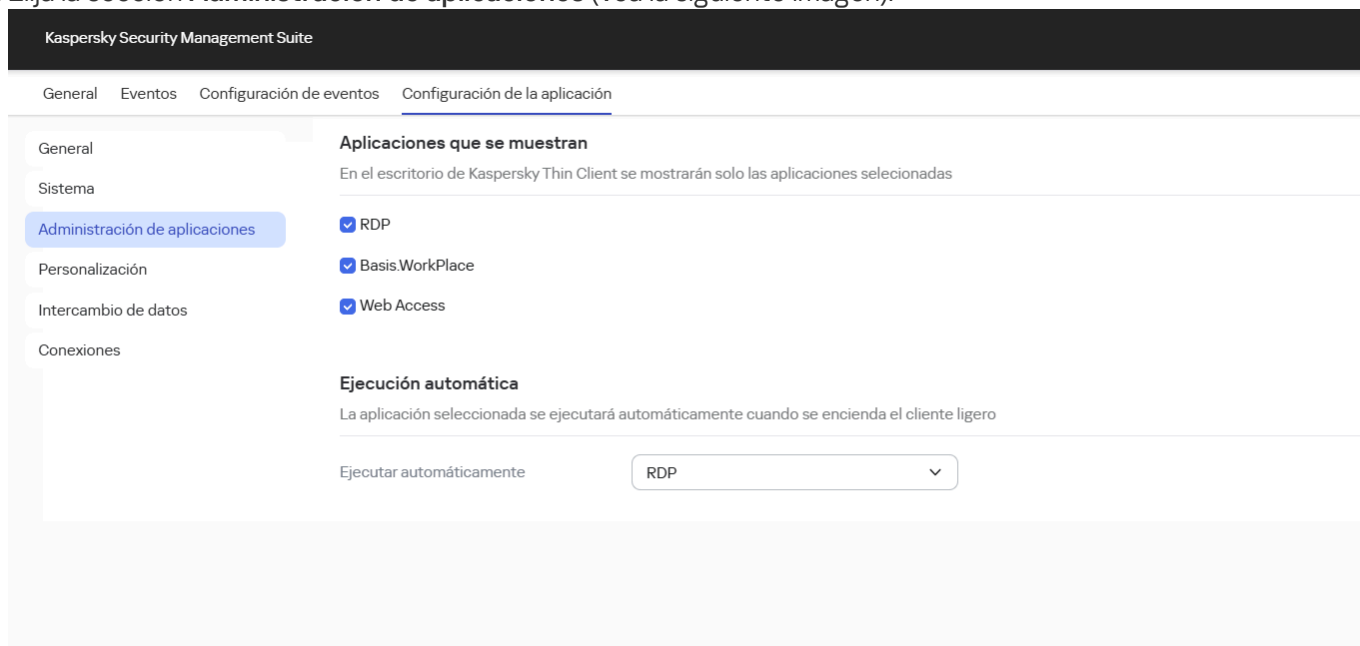
En Web Console, puede seleccionar una [aplicación](#) que se ejecutará automáticamente después de encender el cliente ligero y arrancar el sistema, y puede especificar qué aplicaciones se mostrarán en el escritorio de Kaspersky Thin Client.

Para configurar el inicio automático y la visualización de aplicaciones:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agréguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Elija la sección **Administración de aplicaciones** (vea la siguiente imagen).



Ventana de configuración del inicio automático y la representación gráfica de aplicaciones mediante Web Console

7. En el bloque **Aplicaciones que se muestran**, seleccione las casillas de verificación junto a las aplicaciones que se mostrarán en el escritorio de Kaspersky Thin Client.

En la lista desplegable **Ejecutar automáticamente**, seleccione la aplicación que se ejecutará automáticamente después de encender el dispositivo y arrancar el sistema. Si selecciona **Deshabilitado**, el inicio automático se desactivará.

8. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.

Los cambios se guardan y se aplican al Kaspersky Thin Client instalado en el cliente ligero después de sincronizar Kaspersky Thin Client con Kaspersky Security Center.

Configurar los ajustes de Kaspersky Thin Client para un grupo de administración a través de Web Console

En Web Console, puede usar [directivas](#) para configurar los ajustes de Kaspersky Thin Client instalado en clientes ligeros que estén conectados a Kaspersky Security Center y hayan sido agregados a un [grupo de administración](#).

Configurar los ajustes principales de Kaspersky Thin Client a través de Web Console: grupo de administración

En Web Console puede usar [directivas](#) para asignar nombres a los clientes ligeros incluidos en un [grupo de administración](#) y especificar los datos de contacto del administrador que se mostrarán en la interfaz de Kaspersky Thin Client instalada en estos dispositivos.

Para configurar los ajustes principales de Kaspersky Thin Client para un dispositivo mediante Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a la sección **General** (vea la siguiente imagen).

The screenshot shows the 'Kaspersky Security Management Suite' interface. At the top, there's a navigation bar with tabs: 'General', 'Configuración de eventos', 'Configuración de la aplicación' (which is active), and 'Historial de revisiones'. On the left, a sidebar lists various settings categories: 'General' (highlighted), 'Sistema', 'Administración de aplicaciones', 'Personalización', 'Intercambio de datos', 'Conexiones', and 'Certificados'. The main content area is titled 'Regla de denominación de dispositivos de grupo'. It includes a description: 'Todos los dispositivos del grupo tendrán un nombre compuesto. Ejemplo: Accounting-00000001-Voronezh.' Below this, there are two input fields: 'Nombre' with a placeholder 'Introduzca el nombre' and 'Sufijo' with a placeholder 'Introduzca información adicional', separated by a separator '- Id. del dispositivo -'. Further down, there's a section 'Contactos del Servicio de soporte técnico' with the text 'Los usuarios verán los datos de contacto en la interfaz de Kaspersky Thin Client.' and a 'Datos de contacto' field with a placeholder 'Especifique el número de teléfono y la dirección de correo electrónico del servicio de soporte técnico o del administrador de su empresa'.

Ventana para configurar los ajustes principales de Kaspersky Thin Client instalado en clientes ligeros incluidos en un grupo de administración mediante Web Console

5. Configure los ajustes necesarios:

- En la sección **Regla de denominación de dispositivos de grupo**, ingrese el nombre y la información adicional en los campos correspondientes. Estos datos se muestran en el nombre de cada cliente ligero agregado al grupo de administración. Puede ingresar letras mayúsculas y minúsculas en alfabeto cirílico o latino y caracteres especiales. Longitud máxima del texto en cada campo: 10 caracteres.

Los nombres de los clientes ligeros también incluyen un identificador (ID). Se trata de un conjunto único de ocho caracteres que se genera automáticamente para cada dispositivo agregado al grupo de administración. Puede [cambiar el identificador de un cliente ligero individual](#).

- En la sección **Contactos del Servicio de soporte técnico**, en el campo **Datos de contacto**, introduzca el número de teléfono y el nombre del administrador y otros datos como la dirección de correo electrónico de su servicio de soporte técnico. El campo admite un máximo de ochenta caracteres.

La información ingresada sobre los clientes ligeros agregados al grupo de administración se mostrará en la interfaz de Kaspersky Thin Client: en el panel de control, en las ventanas de confirmación para [restablecer los parámetros y datos de Kaspersky Thin Client](#), en la [confirmación de cambios en los parámetros de conexión con Kaspersky Security Center](#), así como durante el reemplazo del [certificado de conexión con Kaspersky Security Center](#).

6. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.

7. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardarán y se aplicarán a las instancias de Kaspersky Thin Client instaladas en los clientes ligeros que se añadan al grupo de administración después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

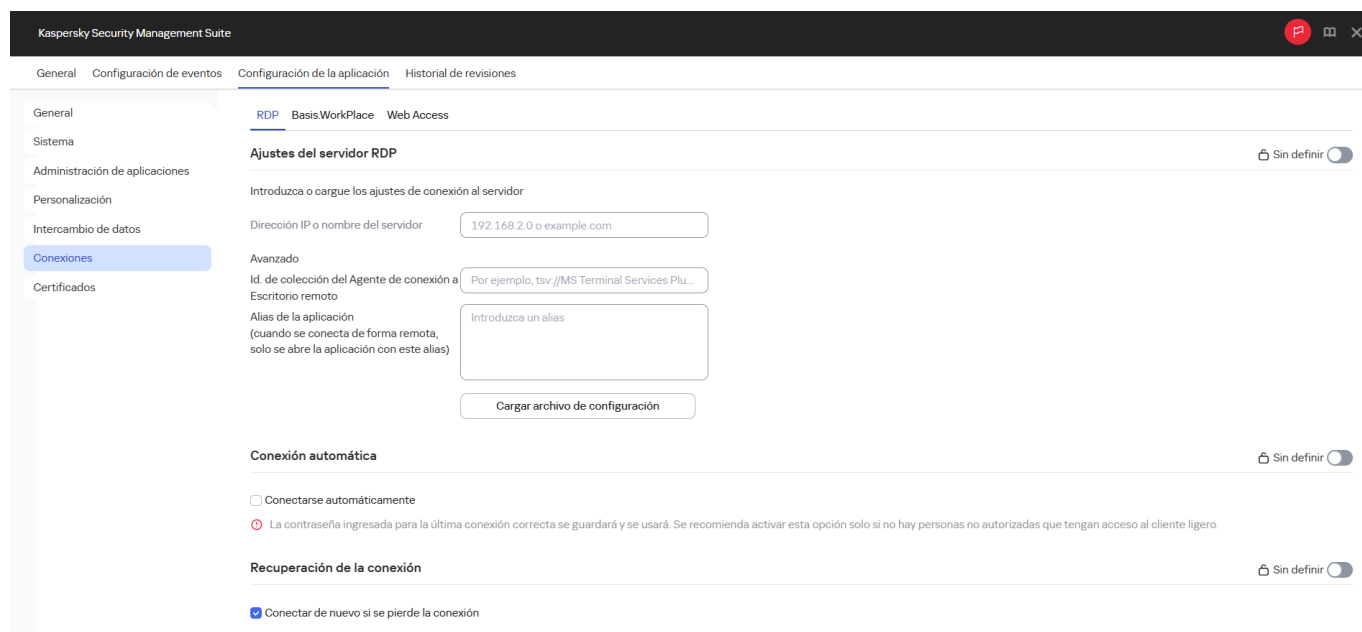
Configurar una conexión a un entorno remoto usando la aplicación RDP a través de Web Console: grupo de administración

En Web Console, puede usar [directivas](#) para configurar los ajustes para [conectarse a un entorno remoto usando la aplicación RDP](#).

Para configurar los ajustes para conectarse a un entorno remoto usando la aplicación RDP:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione **Conexiones** → **RDP**.

Se abre una ventana para configurar los ajustes que se usarán al conectarse al entorno remoto (vea la siguiente imagen).



Ventana para configurar una conexión a un entorno remoto en la aplicación RDP mediante Web Console: grupo de administración

5. En el campo de **dirección IP o nombre del servidor**, ingrese la dirección IP o el nombre del servidor que desee usar para conectarse a un escritorio remoto a través de RDP.
6. Si desea usar el Agente de conexión a Escritorio remoto de Microsoft para conectarse a un escritorio remoto, en el campo **Id. de colección del Agente de conexión a Escritorio remoto**, ingrese el id. de la colección en formato `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` hace referencia al identificador específico de la colección).

Si desea iniciar una aplicación virtual, ingrese el alias de la aplicación en el campo **Alias de la aplicación**.

Si tiene un archivo de configuración que contiene los ajustes para conectarse al Agente de conexión al Escritorio remoto de Microsoft y, si es necesario, el nombre de la aplicación para abrir, haga clic en el botón **Cargar archivo de configuración** y cargue el archivo. En ese caso, no necesitará completar el campo **Id. de colección del Agente de conexión a Escritorio remoto** y **Alias de la aplicación**.

7. Si desea que la conexión se restablezca automáticamente ante una desconexión inesperada, marque la casilla **Conectar de nuevo si se pierde la conexión**.
8. En el bloque de ajustes **Redirección de dispositivos**, seleccione los dispositivos que se redirigirán al entorno remoto: **Tarjetas inteligentes, Unidades de memoria USB, Impresoras y otros dispositivos, Micrófono, Dispositivos de reproducción de audio, Cámara web (video), Escáner**.

El volumen del audio y otros ajustes se controlan desde el entorno remoto.

Para redireccionar dispositivos USB a un escritorio remoto que ejecute el sistema operativo Windows 10, es necesario habilitar los Servicios de Escritorio remoto de Microsoft y permitir la redirección de dispositivos Plug and Play en la configuración de los Servicios de Escritorio remoto. En el caso de Microsoft Windows Server 2016 o 2019, también se deben permitir las conexiones remotas a través de los Servicios de Escritorio remoto y se debe permitir la configuración de reglas de control remoto en los Servicios de Escritorio remoto.

9. En el bloque **Calidad de la imagen**, seleccione las casillas junto a la configuración gráfica del escritorio remoto que desea usar: **Suavizar fuentes**, **Animación de menús**, **Fondo de escritorio**, **Mostrar el contenido de las ventanas al arrastrarlas**, **Tema mejorado**.

Si habilita las opciones gráficas del escritorio remoto, podría verse afectada la velocidad de las operaciones de Kaspersky Thin Client.

10. Si su estación de trabajo tiene dos monitores y desea que la imagen del escritorio remoto se muestre en ambos, marque la casilla **Usar dos monitores** en el bloque **Administración de monitores**.
11. Para mejorar el rendimiento cuando se conecte a aplicaciones o escritorios remotos, en el bloque **Rendimiento**, marque **Mejorar el rendimiento gráfico**.
12. Para conectarse automáticamente a un escritorio remoto o una aplicación virtual cuando se inicie la aplicación RDP, en el bloque **Conexión automática**, seleccione la casilla **Conectarse automáticamente**.
- Para activar esta función, el usuario debe conectarse manualmente y desconectarse del entorno remoto una vez. Cuando lo hace, los siguientes datos para conectarse al servidor RDP se guardan en el almacenamiento del cliente ligero: nombre de usuario, dirección del servidor y contraseña. La siguiente vez que inicie la aplicación RDP, estas credenciales se usarán para iniciar automáticamente una conexión con el entorno remoto. Si deshabilita la función de conexión automática, la contraseña guardada se elimina del almacenamiento del dispositivo.
- Web Console no le permite establecer una contraseña para conectarse a un entorno remoto.
- Para conectarse automáticamente al entorno remoto en la aplicación RDP inmediatamente después de iniciar Kaspersky Thin Client, [configure el inicio automático de la aplicación](#).
13. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.
14. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardarán y se aplicarán a las instancias de Kaspersky Thin Client instaladas en los clientes ligeros que se añadan al grupo de administración después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

Configurar la conexión a un entorno remoto usando la aplicación Basis.WorkPlace a través de Web Console: grupo de administración

En Web Console, puede usar [directivas](#) para configurar los ajustes de [conexión a un entorno remoto desplegado en la infraestructura Basis.WorkPlace](#).

Los usuarios no pueden iniciar un cambio de contraseña en Kaspersky Thin Client.

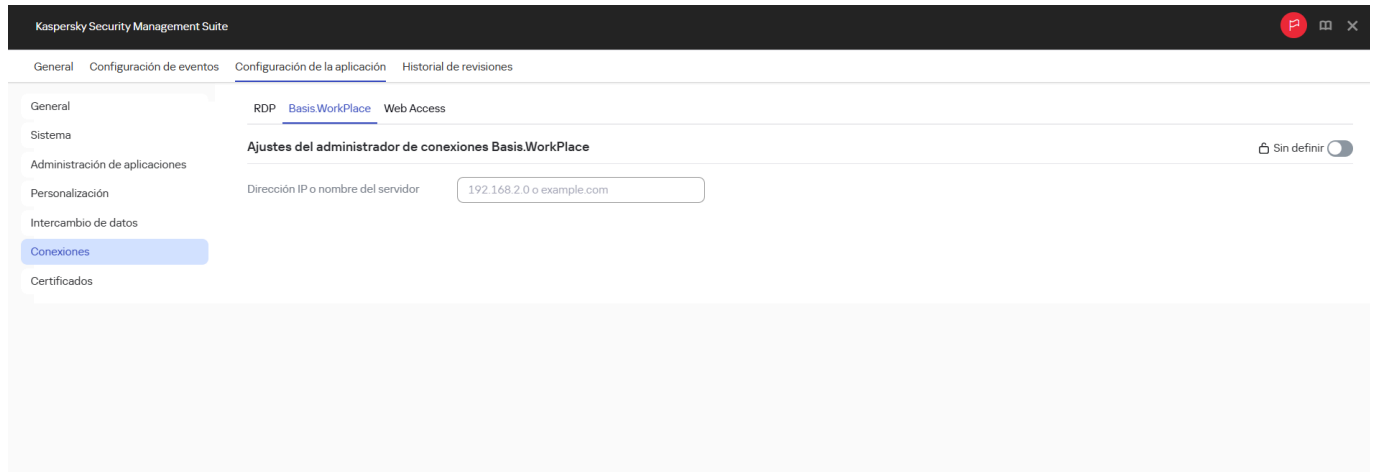
Para configurar los ajustes para conectarse a un entorno remoto desplegado en la infraestructura de Basis.WorkPlace:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.

3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Seleccione **Conexiones** → **Basis.WorkPlace**.

Se abre una ventana para configurar los ajustes que se usarán al conectarse al entorno remoto (vea la siguiente imagen).



Ventana para configurar la conexión a un entorno remoto desplegado en la infraestructura Basis.WorkPlace a través de Web Console: grupo de administración

5. En **Dirección IP o nombre del servidor**, ingrese la dirección IP o el nombre del servidor al que desee conectarse.

6. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.

7. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardarán y se aplicarán a las instancias de Kaspersky Thin Client instaladas en los clientes ligeros que se añadan al grupo de administración después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

Configurar una conexión a un entorno remoto usando la aplicación Web Access a través de Web Console: grupo de administración

En Web Console, puede usar [directivas](#) para configurar los ajustes de [conexión a un entorno remoto usando la aplicación Web Access](#).

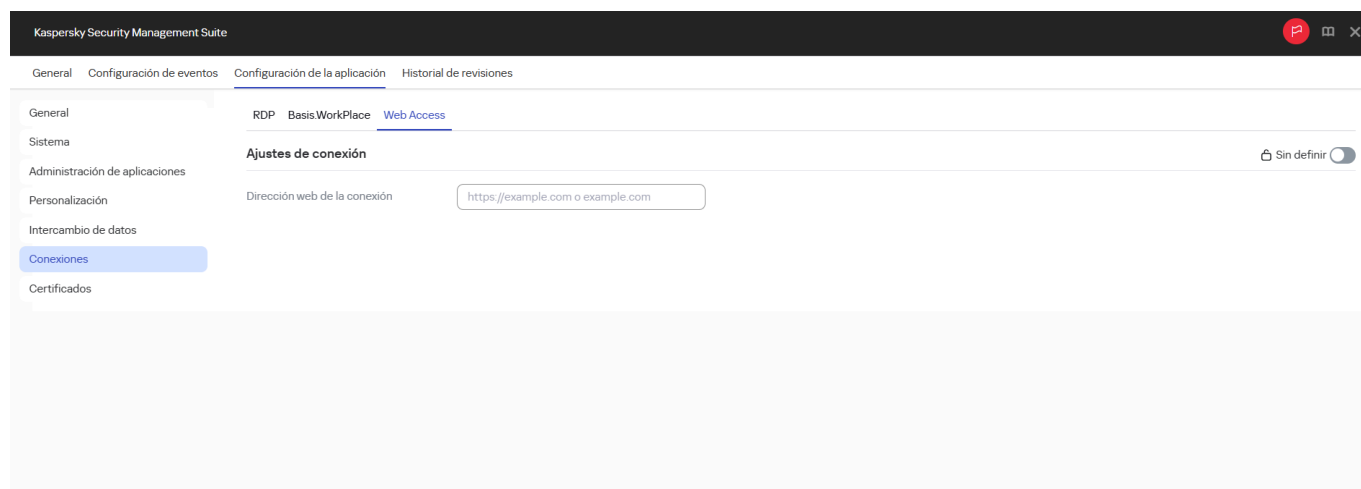
En la aplicación Web Access, puede conectarse a un entorno remoto desplegado en infraestructuras Citrix Workspace. Web Access admite HTML5 y proporciona una conexión HTTPS segura al conectarse.

Para configurar los ajustes para conectarse a un entorno remoto usando la aplicación Web Access:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Seleccione **Conexiones** → **Web Access**.

Se abre una ventana para configurar los ajustes que se usarán al conectarse al entorno remoto (vea la siguiente imagen).



Ventana para configurar una conexión a un entorno remoto en la aplicación Web Access mediante Web Console: grupo de administración

5. En el campo **Dirección web de la conexión**, ingrese la dirección web del servidor que se usará para conectarse al entorno remoto correspondiente.

6. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.

7. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardarán y se aplicarán a las instancias de Kaspersky Thin Client instaladas en los clientes ligeros que se añadan al grupo de administración después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

Configurar los monitores y las pantallas a través de Web Console: grupo de administración

En Web Console, puede usar [las directivas](#) para configurar los monitores conectados a los clientes ligeros y la configuración de las pantallas de Kaspersky Thin Client.

Kaspersky Thin Client permite conectar dos monitores. El sistema considera que uno de los monitores es el principal y el otro, secundario. Durante una [sesión remota](#), el panel de conexión se muestra en la pantalla del monitor principal. La pantalla del monitor secundario amplía o duplica la imagen del monitor principal. En Web Console, puede seleccionar qué monitor debe considerarse el monitor principal (en adelante, también "cambiar el diseño del monitor").

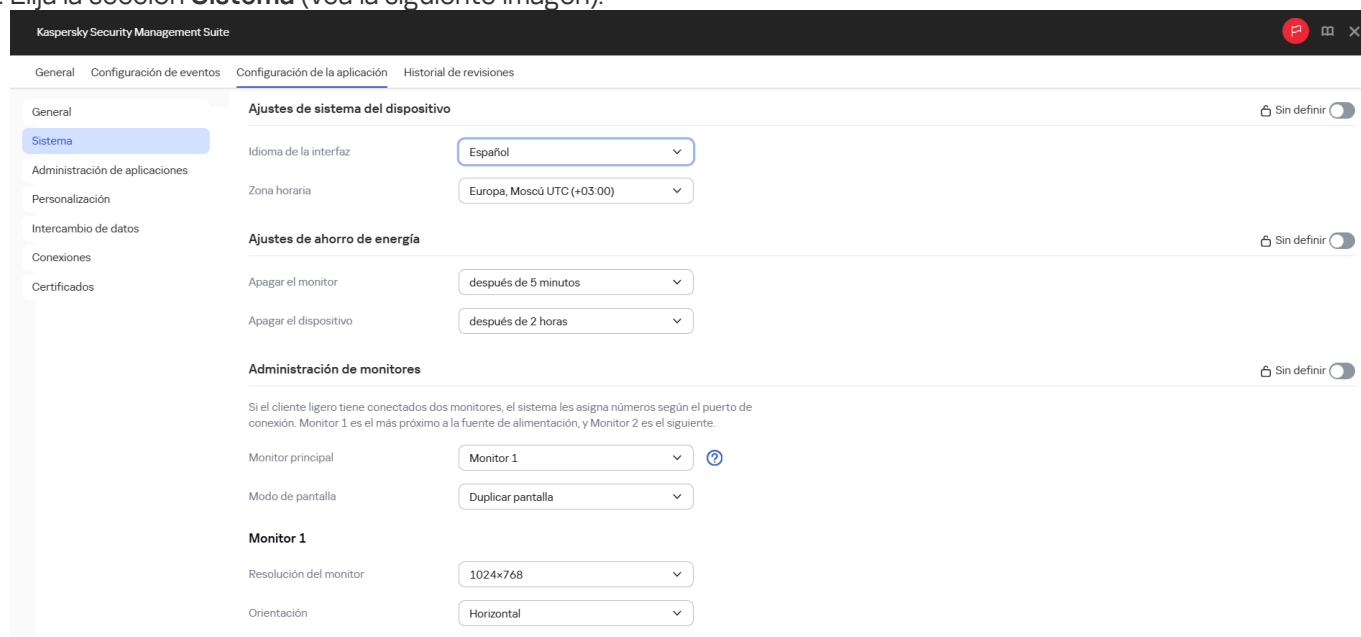
En la interfaz de Web Console, los monitores están numerados. El sistema asigna números a los monitores según el puerto al que estén conectados: el monitor 1 es el conectado al puerto más cercano a la fuente de alimentación y el monitor 2 es el siguiente. Consulte la documentación del fabricante del dispositivo para conocer la ubicación de los puertos en [los modelos de cliente ligero compatibles](#).

Web Console no muestra información sobre cuántos monitores están conectados a un cliente ligero específico.

Si desea que la pantalla de la sesión remota se muestre en ambos monitores, habilítelos en la configuración de conexión del entorno de conexión remota en las aplicaciones [RDP](#) o [Basis.WorkPlace](#).

Para configurar monitores y pantallas mediante Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Sistema** (vea la siguiente imagen).



Ventana para configurar los monitores y las pantallas de un dispositivo mediante Web Console: grupo de administración

5. En el grupo de **Administración de monitores**, configure los ajustes necesarios:

- En la lista desplegable **Monitor principal**, seleccione qué monitor debe considerarse principal.

Si solo hay un monitor conectado a uno de los clientes ligeros del grupo de administración, se aplican los ajustes del monitor configurado como principal en Web Console.

- En la lista desplegable **Modo de pantalla**, seleccione la opción de visualización de imagen:
 - **Extender pantalla**: la imagen se extiende a lo largo de dos monitores.
 - **Duplicar pantalla**: la imagen de la pantalla del monitor principal se duplica en el secundario.
- En la lista desplegable **Resolución del monitor**, seleccione la resolución que desea para la pantalla seleccionada.

Las resoluciones admitidas se enumeran [en la sección de requisitos de hardware y software](#).

Si el valor **Máxima posible** está seleccionado, se establece el valor más alto del parámetro admitido por el monitor y por Kaspersky Thin Client.

- En la lista desplegable **Orientación**, seleccione la posición de la pantalla:
 - **Horizontal**: la posición estándar de la pantalla.
 - **Horizontal invertido**: la pantalla gira 180°.
 - **Vertical**: la pantalla gira 90°.
 - **Vertical invertido**: la pantalla gira 270°.
- 6. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.
- 7. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardarán y se aplicarán a las instancias de Kaspersky Thin Client instaladas en los clientes ligeros que se añadan al grupo de administración después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

Configurar los ajustes de sistema de Kaspersky Thin Client a través de Web Console: grupo de administración

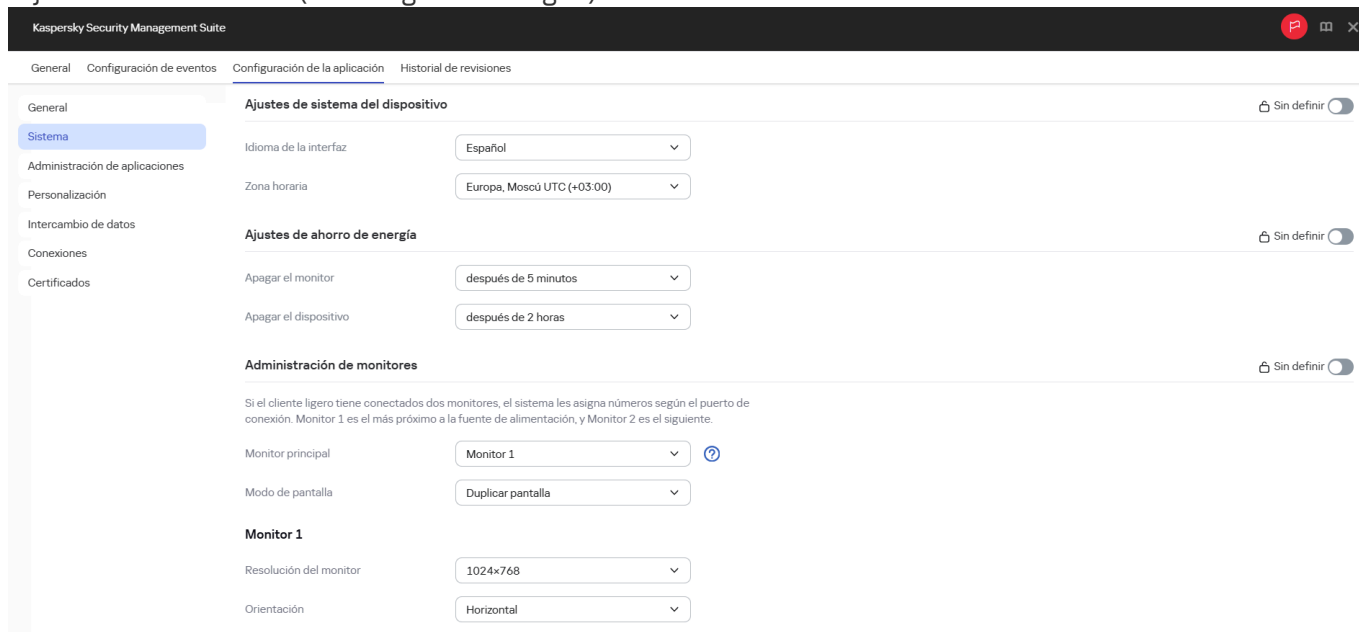
En Web Console, puede usar [directivas](#) para configurar el idioma de la interfaz y la zona horaria de Kaspersky Thin Client, y para configurar la hora de apagado de los clientes ligeros y los monitores que estos tengan conectados.

La interfaz de Kaspersky Thin Client 2.3 está disponible en los siguientes idiomas: ruso, inglés (EE. UU.), español (México) y portugués (Brasil).

Para configurar los ajustes del sistema de Kaspersky Thin Client mediante Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Elija la sección **Sistema** (vea la siguiente imagen).



Ventana para configurar los ajustes del sistema mediante Web Console: grupo de administración

5. En el bloque **Ajustes de sistema del dispositivo**, en las listas desplegables **Idioma de la interfaz** y **Zona horaria**, seleccione los valores pertinentes.

6. En el bloque **Ajustes de ahorro de energía**, configure los siguientes ajustes:

- En la lista desplegable **Apagar el monitor**, seleccione el período de inactividad del sistema después del cual se apagará el monitor.
- En la lista desplegable **Apagar el dispositivo**, seleccione el período de inactividad del sistema después del cual se apagará el cliente ligero.

7. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.

8. Haga clic en el botón **Guardar** en la parte inferior de la página.

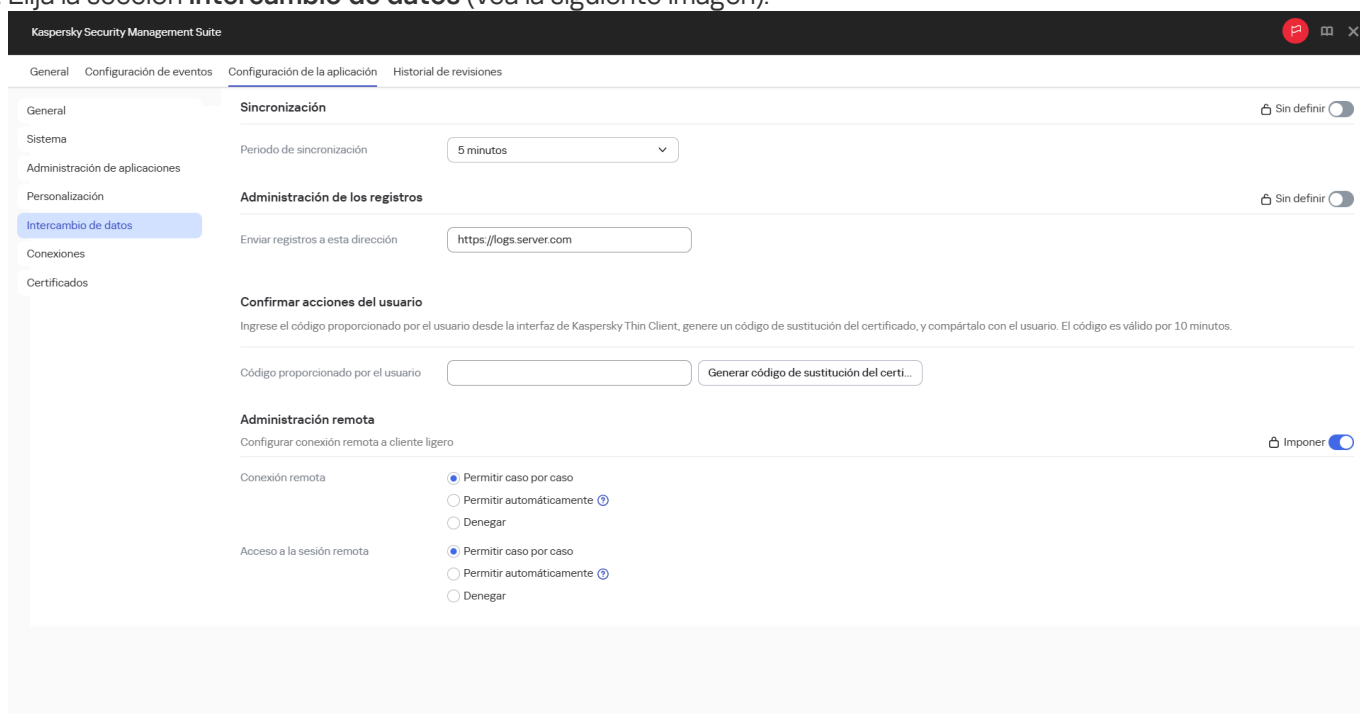
Los cambios se guardarán y se aplicarán a las instancias de Kaspersky Thin Client instaladas en los clientes ligeros que se añadan al grupo de administración después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

Configurar el envío de los registros de Kaspersky Thin Client a un servidor de registros: grupo de administración

En Web Console, puede usar [directivas](#) para cambiar la dirección del [servidor de registros](#) al que se reenvían los [registros de auditoría y de eventos](#) de Kaspersky Thin Client.

Para configurar el reenvío de registros de eventos y registro de auditoría a un servidor de registros mediante Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Intercambio de datos** (vea la siguiente imagen).



Ventana para configurar el envío de los registros de Kaspersky Thin Client para un dispositivo mediante Web Console: grupo de administración

5. En el campo **Enviar registros a esta dirección**, ingrese la dirección del servidor de registros de destino en formato `https://<dirección del servidor>`.

Para recibir registros de eventos y registro de auditoría de Kaspersky Thin Client, su organización debe tener implementado un servidor de registros que cumpla con los [requisitos de hardware y software](#).

6. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.
7. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardarán y se aplicarán a las instancias de Kaspersky Thin Client instaladas en los clientes ligeros que se añadan al grupo de administración después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

Personalizar Kaspersky Thin Client: grupo de administración

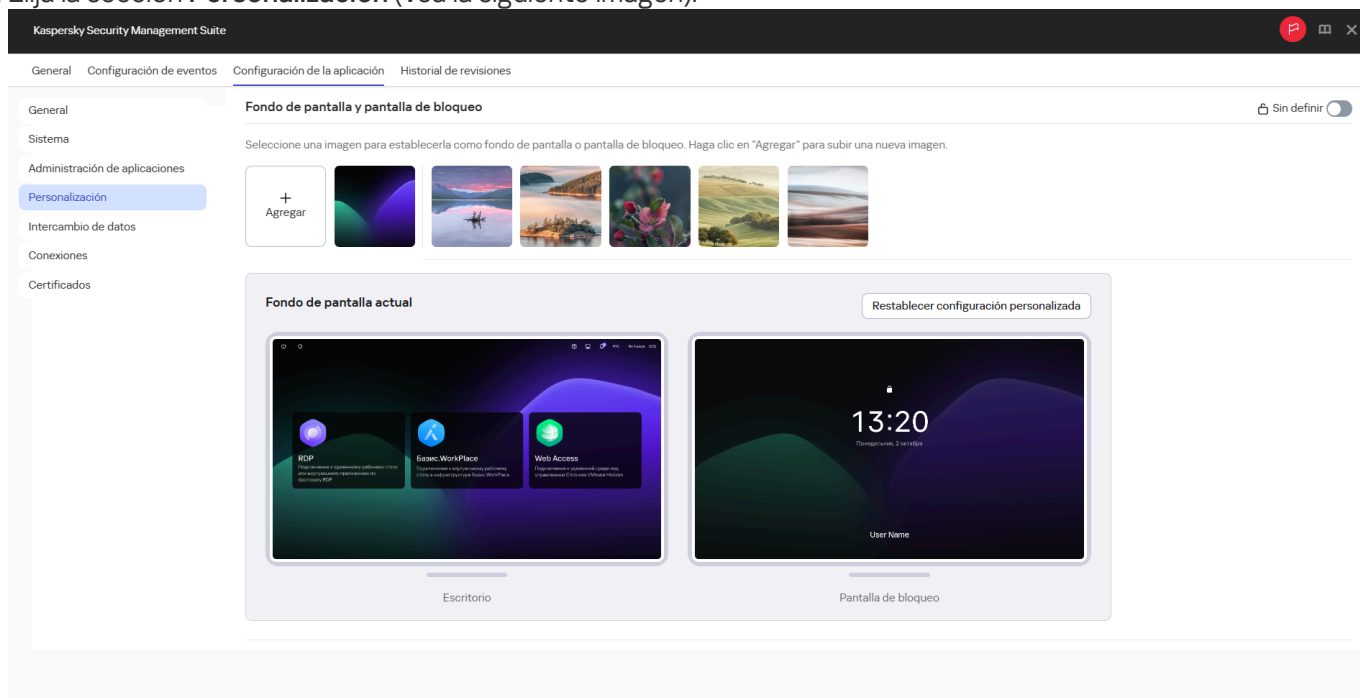
En Web Console, puede usar [directivas](#) para cargar sus imágenes y establecerlas como fondo de escritorio o pantalla de bloqueo de Kaspersky Thin Client. Se admiten los formatos de archivo JPEG, PNG y JPG. El tamaño máximo que puede tener cada archivo es de 15 MB. De ser necesario, puede eliminar las imágenes que haya cargado a través de Web Console.

De manera predeterminada, el escritorio y la pantalla de bloqueo de Kaspersky Thin Client tienen un fondo estándar. Si ha configurado un fondo, puede restablecer su configuración personalizada y restaurar la imagen predeterminada.

No puede cambiar el fondo en la interfaz de Kaspersky Thin Client. Puede cambiar el fondo de las pantallas solo a través de Web Console. La imagen configurada a través de Web Console también cambia al fondo estándar [si se realiza el restablecimiento a la configuración de fábrica](#).

Para cambiar el fondo del escritorio o de la pantalla de bloqueo de Kaspersky Thin Client a través de Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Personalización** (vea la siguiente imagen).



Ventana para configurar la personalización de Kaspersky Thin Client de un dispositivo mediante Web Console.

5. Para cambiar el fondo del escritorio o de la pantalla de bloqueo, siga estos pasos:

a. Seleccione la imagen que desee usar de fondo.

- Si desea cargar una nueva imagen a Web Console, haga clic en el botón **Agregar**.

En la ventana que se abre, arrastre la imagen deseada al área de carga o haga clic en **Cargar un archivo o arrástrelo y suéltelo aquí**. A continuación, en la ventana que aparezca, seleccione la imagen que desee.

- Si desea usar una imagen que ya se haya cargado en Web Console, haga clic en la miniatura de la imagen.

Aparecerá una ventana para previsualizar dónde se ubicará la imagen seleccionada en las pantallas de Kaspersky Thin Client.

Si desea guardar la imagen en Web Console sin establecerla como fondo, vaya al paso c. de estas instrucciones.

b. Marque las casillas adyacentes a las pantallas en las que desee usar la imagen como fondo:

- **Escritorio:** la imagen se establecerá como [fondo de escritorio de Kaspersky Thin Client](#).
- **Pantalla de bloqueo:** la imagen se establecerá como [fondo de la pantalla de bloqueo](#).

c. Haga clic en **Guardar** en la ventana de previsualización.

Se mostrará la pantalla principal de la sección **Personalización**. Se cambiará el fondo de las pantallas seleccionadas.

6. Para eliminar una imagen cargada en Web Console, ubique el cursor sobre la miniatura de la imagen y haga clic en el botón  que aparecerá.

Confirme sus acciones en la ventana que aparecerá.

La imagen se eliminará de Web Console permanentemente. Si se ha establecido una imagen como fondo en alguna pantalla, se la cambiará por el fondo estándar.

7. Para restaurar el fondo estándar en todas las pantallas, haga clic en **Restablecer configuración personalizada** y confirme sus acciones en la ventana que se abrirá.

8. Se pondrá un fondo estándar en el escritorio y en la pantalla de bloqueo de Kaspersky Thin Client.

9. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.

10. Haga clic en el botón **Guardar** en la parte inferior de la sección **Personalización**.

Los cambios se guardarán y se aplicarán a los clientes ligeros agregados al grupo de administración en el plazo de una hora después de la sincronización de Kaspersky Security Center con Kaspersky Thin Client.

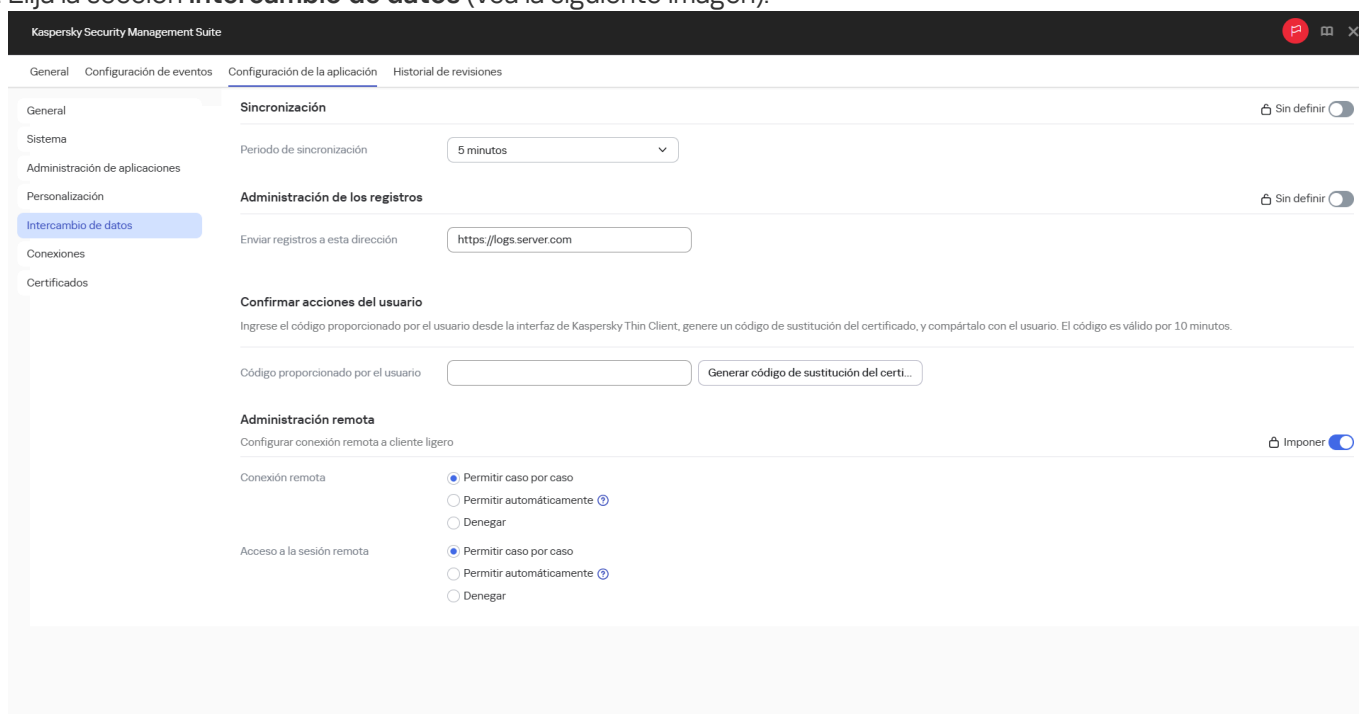
Configurar una conexión remota a un cliente ligero mediante Web Console: grupo de administración

En Web Console, puede usar [directivas](#) para configurar los siguientes ajustes de conexión remota:

- Modo de acceso a la administración remota: determina las condiciones y el procedimiento para conectarse al cliente ligero.
- Modo de acceso a la sesión remota que esté activa en el cliente ligero al establecer conexión con él (en lo sucesivo, para referirse a esta sesión, también se usará el término "pantalla del entorno remoto").
Puede restringir el acceso a la pantalla del entorno remoto si el usuario del cliente ligero trabaja con datos confidenciales o privados.

Si desea configurar los ajustes para la conexión remota de un cliente ligero:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Intercambio de datos** (vea la siguiente imagen).



Ventana para configurar una conexión remota a un cliente ligero mediante Web Console: grupo de administración

5. En la sección **Administración remota**, seleccione el modo de acceso a la capacidad de administración remota del cliente ligero:

- **Permitir automáticamente**

Si selecciona este modo, el administrador podrá conectarse al cliente ligero remoto después de que el usuario [acepte la solicitud de administración remota en la interfaz de Kaspersky Thin Client](#). Si el usuario rechaza la solicitud, la conexión se finalizará. Si no hay respuesta en 30 segundos, la conexión se establece automáticamente.

- **Permitir caso por caso**

En este modo, el administrador podrá conectarse de forma remota al cliente ligero solo después de que el usuario [acepte la solicitud de administración remota en la interfaz de Kaspersky Thin Client](#). Si el usuario rechaza la solicitud, la conexión se finalizará.

- **Denegar**

Si selecciona este modo, el administrador no podrá conectarse al cliente ligero remoto.

Si selecciona los modos **Permitir automáticamente** o **Permitir caso por caso**, se desbloqueará el grupo de opciones **Acceso a la sesión remota**.

6. En el grupo de opciones **Acceso a la sesión remota**, seleccione el modo de acceso a la pantalla del entorno remoto:

- **Permitir automáticamente**

Si selecciona este modo, tras conectarse al cliente ligero, el administrador podrá acceder a la pantalla del entorno remoto sin que el usuario confirme la acción.

- **Permitir caso por caso**

Si selecciona este modo, tras conectarse al cliente ligero, el administrador podrá acceder a la pantalla del entorno remoto únicamente si el usuario [acepta la solicitud de acceso en la interfaz de Kaspersky Thin Client](#).

- **Denegar**

Si selecciona este modo, el administrador no podrá administrar el cliente ligero a distancia hasta que el usuario cierre manualmente su sesión remota.

7. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.

8. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardarán y se aplicarán a las instancias de Kaspersky Thin Client instaladas en los clientes ligeros que se añadan al grupo de administración después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

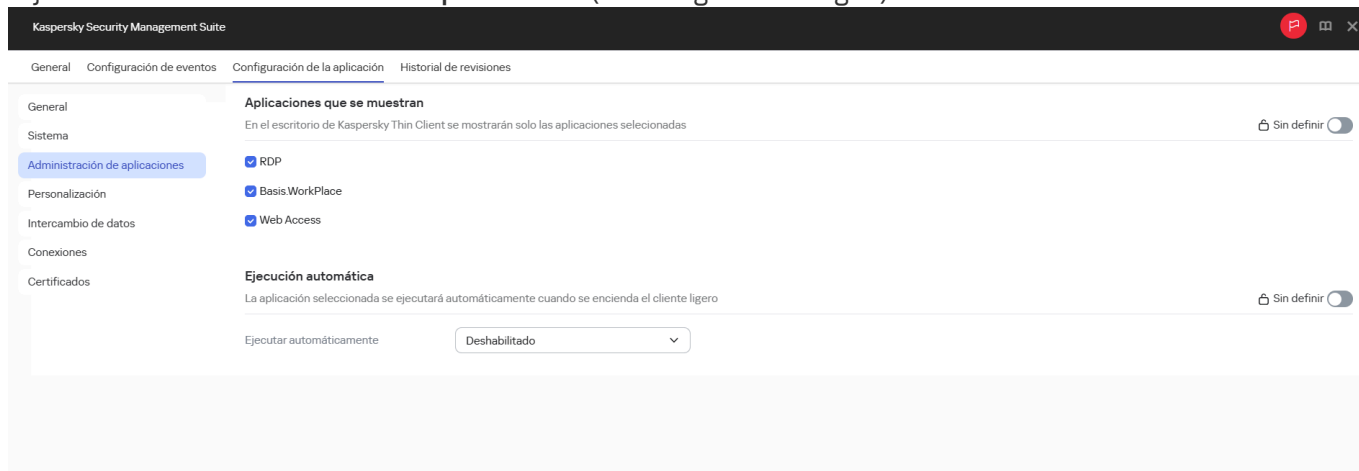
Configurar el inicio automático y la visualización de aplicaciones: grupo de administración

En Web Console, puede usar [directivas](#) para seleccionar una [aplicación](#) que se ejecutará automáticamente después de iniciar el dispositivo y el sistema, y puede especificar qué aplicaciones se mostrarán en el escritorio de Kaspersky Thin Client.

Para configurar el inicio automático y la visualización de aplicaciones:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Elija la sección **Administración de aplicaciones** (vea la siguiente imagen).



Ventana de configuración del inicio automático y la visualización de aplicaciones mediante Web Console

5. En el bloque **Aplicaciones que se muestran**, seleccione las casillas de verificación junto a las aplicaciones que se mostrarán en el escritorio de Kaspersky Thin Client.

En la lista desplegable **Ejecutar automáticamente**, seleccione la aplicación que se ejecutará automáticamente después de encender el dispositivo y arrancar el sistema. Si selecciona **Deshabilitado**, el inicio automático se desactivará.

6. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.

7. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardarán y se aplicarán a las instancias de Kaspersky Thin Client instaladas en los clientes ligeros que se añadan al grupo de administración después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

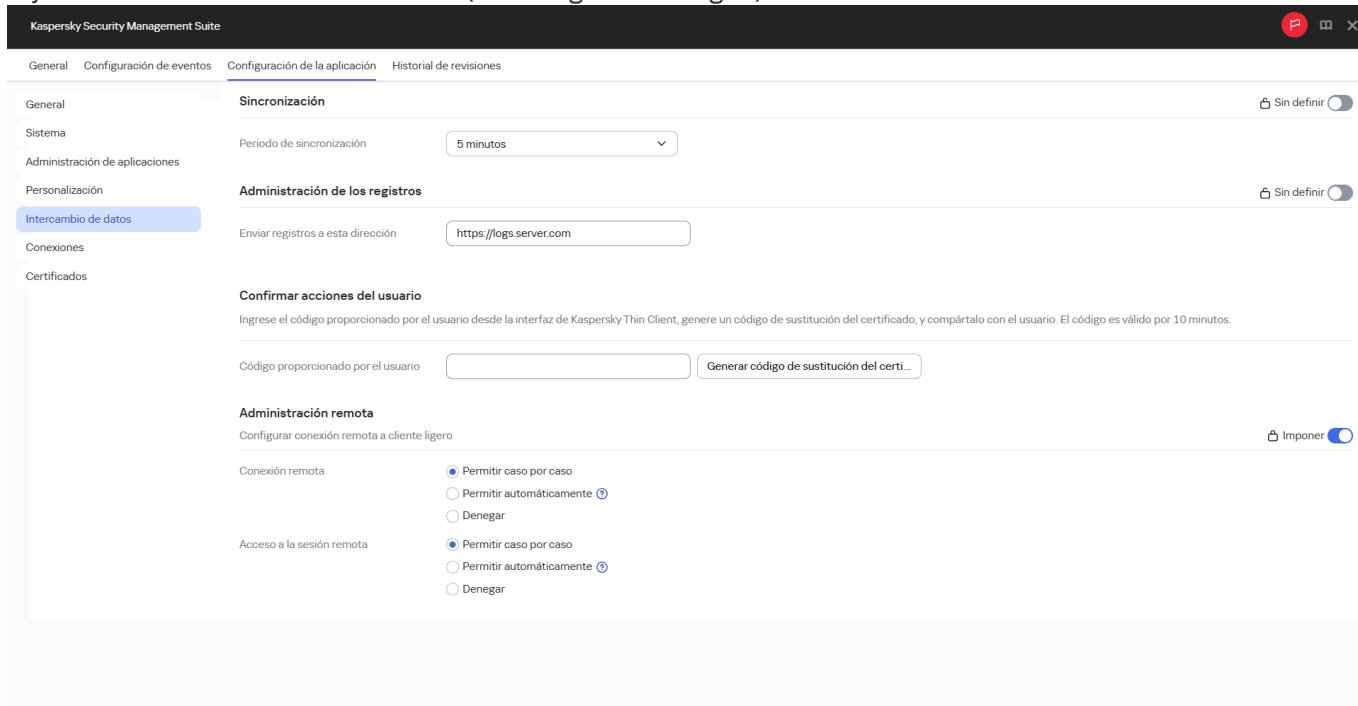
Configurar la sincronización entre Kaspersky Thin Client y Kaspersky Security Center

En Web Console, la única forma de configurar el período de sincronización entre Kaspersky Thin Client y Kaspersky Security Center son las [directivas](#).

Para configurar la sincronización entre Kaspersky Thin Client y Kaspersky Security Center:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.

4. Elija la sección **Intercambio de datos** (vea la siguiente imagen).



Ventana para configurar la sincronización entre Kaspersky Thin Client y Kaspersky Security Center

5. En la lista desplegable **Periodo de sincronización**, defina la frecuencia con la que se realizará la sincronización entre Kaspersky Thin Client y Kaspersky Security Center.
6. Si desea que la configuración establecida se aplique a Kaspersky Thin Client instalado en los grupos de administración secundarios y que no esté disponible para su edición en Kaspersky Thin Client del grupo de administración actual, mueva los [interruptores situados junto a los bloques de configuración correspondientes](#) a la posición **Imponer**.
7. Haga clic en el botón **Guardar** en la parte inferior de la página.

Los cambios se guardarán y se aplicarán a las instancias de Kaspersky Thin Client instaladas en los clientes ligeros que se añadan al grupo de administración después de la sincronización de Kaspersky Thin Client con Kaspersky Security Center.

Confirmar las acciones del usuario de Kaspersky Thin Client

El administrador de Kaspersky Security Center debe confirmar las siguientes acciones de los usuarios:

- [modificación de los ajustes de conexión a Kaspersky Security Center](#)
- [sustitución de los certificados para conectarse a Kaspersky Security Center](#)
- [restablecimiento de todos los ajustes y datos del cliente ligero](#)

Si el cliente ligero con Kaspersky Thin Client no está conectado a Kaspersky Security Center (o si lo está, pero no se lo ha incluido en el [grupo de administración](#)), las solicitudes para confirmar las acciones enumeradas arriba no se enviarán al administrador. [Agregue el cliente ligero al grupo de administración](#) para recibir solicitudes de confirmación de las acciones del usuario.

Para confirmar las modificaciones en los ajustes de conexión a Kaspersky Security Center o restablecer los ajustes de Kaspersky Thin Client:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
2. En la lista que aparece, haga clic en el nombre del cliente ligero correspondiente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#). Si no ve el nombre del cliente ligero en la lista, [agréguelo a un grupo de administración](#).

Si un ajuste que esté configurando está bloqueado [en una directiva que se creó para un grupo de administración](#), no puede cambiar este ajuste al configurar el dispositivo individual. [Cambie](#) o [desbloquee](#) esta configuración en la directiva.

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.
Se abre una ventana con información sobre Kaspersky Thin Client.
5. Seleccione la pestaña **Configuración de la aplicación**.
6. Seleccione la sección **Intercambio de datos**.
7. En el bloque **Confirmar acciones del usuario**, ingrese el código de la interfaz de Kaspersky Thin Client que le haya enviado el usuario. A continuación, haga clic en **Generar código de confirmación**.
Se creará un código de confirmación y se lo mostrará en el bloque **Confirmar acciones del usuario**.
8. Envíe el código de confirmación al usuario de Kaspersky Thin Client.

Para confirmar la sustitución del certificado para conectarse a Kaspersky Security Center:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Seleccione la sección **Intercambio de datos**.
5. En el bloque **Confirmar acciones del usuario**, ingrese el código de la interfaz de Kaspersky Thin Client que le haya enviado el usuario. A continuación, haga clic en **Generar código de sustitución del certificado**.
Se creará un código de sustitución del certificado y se lo mostrará en el bloque **Confirmar acciones del usuario**.
6. Envíe el código de sustitución del certificado al usuario de Kaspersky Thin Client.

Administrar los certificados de Kaspersky Thin Client a través de Web Console

En Kaspersky Security Center, puede acceder a funciones para administrar los [certificados](#) que permiten conectar los clientes ligeros a un servidor de registros o a un entorno remoto. En la interfaz de Kaspersky Security Center Web Console, puede ver, [agregar](#) y [eliminar](#) esos certificados.

Recomendamos configurar la [conexión de los clientes ligeros en el grupo de administración](#) a un servidor de registro y a un entorno remoto utilizando solo los certificados asignados por el administrador en la Consola web. Esto ayudará a evitar que Kaspersky Thin Client se conecte a nodos que no sean de confianza.

Esta sección también proporciona [instrucciones sobre cómo administrar certificados para conectar Kaspersky Thin Client a Kaspersky Security Center](#).

Acerca de los certificados para conectar Kaspersky Thin Client a Kaspersky Security Center

Kaspersky Thin Client utiliza un *certificado móvil de usuario* (en adelante, también denominado "certificado") para conectarse a Kaspersky Security Center. Para obtener información detallada sobre este y otros tipos de certificados utilizados por Kaspersky Security Center, consulte la [Ayuda en línea de Kaspersky Security Center](#).

Este certificado se crea a través del *asistente de inicio rápido del Servidor de administración* cuando concluye la instalación de Kaspersky Security Center. Por defecto, el certificado emitido tiene una validez de un año.

Los certificados móviles de usuario no se vuelven a emitir automáticamente.

Puede volver a [emitir el certificado en Web Console](#) o [crear un nuevo certificado](#) manualmente y [cargarlo en Web Console](#).

Al [migrar a un nuevo Servidor de administración de Kaspersky Security Center](#), cree manualmente un nuevo [certificado](#) para cargarlo al Servidor actual como certificado de reserva y luego al nuevo Servidor como certificado principal.

Emitir de nuevo un certificado para conectar Kaspersky Thin Client a Kaspersky Security Center mediante Web Console

Kaspersky Thin Client utiliza un certificado móvil de usuario para conectarse con Kaspersky Security Center. Los certificados de este tipo no se vuelven a emitir automáticamente.

Para volver a emitir un certificado para conectar Kaspersky Thin Client a Kaspersky Security Center en la interfaz de Web Console:

1. En el menú de Kaspersky Security Center Web Console, haga clic en el botón  junto al nombre del servidor de administración de Kaspersky Security Center.
Se abre la ventana **Propiedades del Servidor de administración**.
2. Elija la subsección **Certificados**.
3. En la ventana que se abre, en la sección **Autenticación del Servidor de administración por dispositivos móviles**, seleccione el certificado requerido y haga clic en **Emitir nuevamente**.
4. En la ventana que se abre, especifique la dirección del servidor e indique cuándo activar el certificado. Confirme su elección.
5. Haga clic en **Guardar** en la ventana que se abre.

El certificado para conectar Kaspersky Thin Client a Kaspersky Security Center se ha reemitido.

Los dispositivos administrados y los dispositivos incluidos en un [grupo de administración](#) recibirán el certificado reemitido para conectarse a Kaspersky Security Center cuando Kaspersky Thin Client se sincronice con Kaspersky Security Center. El certificado reemitido se guarda en el almacenamiento de certificados de Kaspersky Thin Client y se puede usar como certificado de reserva para conectar clientes ligeros a Kaspersky Security Center cuando caduque el certificado vigente.

También puede [emitir manualmente un nuevo certificado para conectar Kaspersky Thin Client a Kaspersky Security Center](#).

Crear un certificado de usuario para conectar Kaspersky Thin Client a Kaspersky Security Center

También puede crear [un certificado](#) para conectar Kaspersky Thin Client a Kaspersky Security Center. El certificado creado se puede usar como principal o de reserva, por ejemplo, al [migrar a un nuevo Servidor de administración de Kaspersky Security Center](#).

Le recomendamos que se familiarice con los requisitos del certificado de Kaspersky Security Center [en la Ayuda en línea de Kaspersky Security Center](#).

El certificado creado debe [cargarse en Web Console](#).

Para crear un certificado para conectar Kaspersky Thin Client a Kaspersky Security Center con la herramienta OpenSSL:

1. Abra la consola y vaya a la carpeta en la que desee crear el certificado.
2. En la consola, inicie la herramienta OpenSSL y ejecute el siguiente comando:

```
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"
```

donde:

- `-keyout key.pem` es el nombre del archivo en el que se guardará la clave privada del certificado creado.
- `-out server.pem` es el nombre del archivo en el que se guardará el certificado creado.
- `-days` es un parámetro que define el plazo de validez, en días, del certificado creado. Recomendamos que el plazo de validez del certificado no sea superior a 397 días.
- `-subj '/CN=mydomain.ru/C=RU/L=Moscow/O=My Organization Name/OU=My Organization Unit Name'` son datos de su organización: nombre de dominio, ubicación y nombre.

3. Ingrese y confirme la contraseña para la clave privada del certificado. Deberá introducir esta contraseña cuando cargue el certificado de usuario como certificado para dispositivos móviles en Web Console. Longitud mínima de la contraseña: 8 caracteres.

Como resultado, se crearán los siguientes dos archivos en la carpeta en la que haya ejecutado el comando:

- `server.pem`, el archivo del certificado para conectar Kaspersky Thin Client a Kaspersky Security Center.
- `key.pem`, la clave privada del certificado para conectar Kaspersky Thin Client a Kaspersky Security Center.

Subir un certificado para conectar Kaspersky Thin Client a Kaspersky Security Center mediante Web Console

Después de [crear un certificado](#) para conectar Kaspersky Thin Client a Kaspersky Security Center, cargue este certificado en Web Console para transferirlo a los clientes ligeros agregados al [grupo de administración](#).

Le recomendamos que se familiarice con los requisitos del certificado de Kaspersky Security Center [en la Ayuda en línea de Kaspersky Security Center](#).

Para cargar en Web Console un certificado para conectar Kaspersky Thin Client a Kaspersky Security Center:

1. En el menú de Kaspersky Security Center Web Console, haga clic en el botón  junto al nombre del Servidor de administración de Kaspersky Security Center.

Se abre la ventana **Propiedades del Servidor de administración**.

2. Elija la subsección **Certificados**.

3. En la ventana que se abre, en el bloque **Autenticación del Servidor de administración por dispositivos móviles**, seleccione **Otro certificado** y haga clic en el botón **Administrar certificado**.

4. En el panel que se abre a la derecha, haga clic en **Examinar** y realice las siguientes acciones:

5. En la lista desplegable **Tipo de certificado**, seleccione **certificado X.509**:

- a. Si el certificado de usuario está protegido con contraseña, ingrese la contraseña.
- b. Haga clic en el botón **Examinar** del bloque **Certificado** y seleccione el archivo del certificado de usuario.
- c. Haga clic en el botón **Examinar** del bloque **Clave privada** y seleccione la clave privada del certificado de usuario.

6. Haga clic en **Guardar** para guardar el certificado que desea agregar.

7. Haga clic en **Guardar** para guardar los cambios realizados en la subsección **Certificados**.

El certificado para conectar Kaspersky Thin Client a Kaspersky Security Center se cargará en Web Console. Los dispositivos incluidos en el grupo de administración reciben el nuevo certificado después de que Kaspersky Thin Client se sincroniza con Kaspersky Security Center.

Agregar nuevos certificados en Web Console

En Web Console, puede agregar [certificados](#) para conectarse a un entorno remoto o a un servidor de registros. Para hacerlo, el cliente ligero se debe [agregar a un grupo de administración](#).

Cuando se agrega un certificado para un cliente ligero en Web Console, todos los certificados aceptados antes por el usuario se eliminan del almacén de certificados del dispositivo.

Para agregar nuevos certificados a través de Web Console:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Certificados**.
5. En la parte superior de la tabla **Certificados válidos**, haga clic en el botón **Agregar**.
6. En el panel que se abre a la derecha, seleccione todos los certificados que se hayan cargado anteriormente y seleccione los nuevos certificados. El tamaño total de los archivos cargados no debe ser superior a 1 MB. Los certificados deben estar en formato DER. Cada archivo de certificado debe contener un solo certificado. De ser necesario, puede [convertir sus certificados de formato PEM a DER](#) por adelantado.
7. Haga clic en **Aceptar** para confirmar la carga de los certificados seleccionados.

Los certificados seleccionados se cargarán y se agregará información sobre ellos en la tabla **Certificados válidos**.

Si el certificado agregado es un certificado raíz, la conexión solo podrá establecerse utilizando el nombre de dominio del servidor.

Eliminar certificados de Web Console

En Web Console, puede eliminar los certificados que se asignaron a los clientes ligeros en un [grupo de administración](#).

Si elimina todos los certificados [asignados a un grupo de clientes ligeros](#), los dispositivos de dicho grupo podrán conectarse a cualquier servidor, incluidos aquellos que no tengan asignado ningún certificado.

Para eliminar certificados:

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el [nombre de la directiva](#) del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Certificados**.
5. En la tabla **Certificados válidos**, marque las casillas ubicadas junto a los certificados que desee eliminar.
6. Haga clic en **Eliminar** y confirme la eliminación.

Se eliminarán los certificados seleccionados.

Convertir un certificado del formato PEM al formato DER

Kaspersky Security Management Suite solo permite cargar certificados en formato DER. Puede convertir un archivo de certificado del formato PEM al formato DER.

Para llevar a cabo estas instrucciones en una computadora local, debe contar con la herramienta OpenSSL.

Para convertir un archivo de certificado del formato PEM al formato DER:

1. Inicie la consola en una computadora local.
2. Vaya a la carpeta que contenga el archivo del certificado en formato PEM y ejecute el siguiente comando para convertir el archivo:

```
openssl x509 -outform der -in <nombre del archivo del certificado>.pem -out <nombre del archivo del certificado>.der
```

donde:

- <nombre del archivo del certificado>.pem es el nombre del archivo del certificado original en formato PEM.
- <nombre del archivo del certificado>.der es el nombre del archivo del certificado convertido al formato DER.

El archivo del certificado en formato DER se generará en la misma carpeta.

Actualizar un certificado al migrar a un nuevo servidor de Kaspersky Security Center

Para [migrar clientes ligeros a un nuevo Servidor de administración de Kaspersky Security Center](#), emita un [certificado](#), guárdelo en el Servidor de Kaspersky Security Center actual como uno de reserva y luego utilícelo en el nuevo Servidor como certificado principal.

Para emitir y preparar un nuevo certificado:

1. Abra la consola y vaya a la carpeta en la que desee crear el certificado.
2. Ejecute la utilidad OpenSSL y emita el certificado con el siguiente comando:

```
openssl req -x509 -sha256 -nodes -days 397 -newkey rsa:2048 -keyout <nombre del archivo de clave>.key -out <nombre del archivo de certificado>.crt
```

El certificado generado y los archivos de clave se guardan localmente.

3. Empaquete el certificado y la clave en un contenedor usando el siguiente comando:

```
openssl pkcs12 -export -out <nombre del contenedor>.pfx -inkey <nombre del archivo de clave>.key -in <nombre del archivo de certificado>.crt
```
4. Ingrese y repita la contraseña del contenedor. Esta contraseña es necesaria para cargar el certificado en los servidores.

Como resultado, el archivo de contenedor en formato PFX se guarda localmente.

Para cargar un certificado en el servidor de Kaspersky Security Center actual como uno de reserva:

1. Vaya a la carpeta donde está instalado Kaspersky Security Center e inicie la consola.
2. Ejecute la utilidad klsetsrvcert e ingrese el siguiente comando:

```
klsetsrvcert -t MR -i <ruta al contenedor> -p <contraseña del contenedor> -o NoCA
```

No es necesario que descargue la utilidad klsetsrvcert. La utilidad está incluida en el kit de distribución de Kaspersky Security Center.

Tras ejecutarse el comando, Kaspersky Security Center se reinicia.

El [certificado de reserva](#) se carga en Web Console.

Para cargar el certificado en un nuevo servidor de Kaspersky Security Center como principal:

En la consola, inicie la utilidad klsetsrvcert y ejecute el siguiente comando:

```
klsetsrvcert -t M -i <ruta al contenedor> -p <contraseña del contenedor> -o NoCA
```

Una vez ejecutadas estas instrucciones, el certificado para conectarse al nuevo Servidor de administración de Kaspersky Security Center se actualiza.

Supervisar los eventos de Kaspersky Thin Client a través de Kaspersky Security Center Web Console

En esta sección, encontrará instrucciones para monitorear los eventos registrados en Kaspersky Thin Client a través de Kaspersky Security Center Web Console.

Configurar el registro de notificaciones de eventos de Kaspersky Thin Client a través de Kaspersky Security Center Web Console

Kaspersky Security Center permite recibir información sobre los eventos que suceden mientras Kaspersky Thin Client está en ejecución. Mediante la interfaz de Kaspersky Security Center Web Console, puede configurar una notificación sobre el registro de estos eventos. En Kaspersky Security Center, cada evento tiene su propio nivel de importancia. Dependiendo de las circunstancias en las que ocurre, a un evento se le puede asignar uno de los siguientes niveles de importancia:

- Un evento *crítico* es un evento que se registra cuando ocurre un problema de extrema gravedad, que puede derivar en pérdidas de información, en un error crítico o en un fallo de funcionamiento.
- Un *error funcional* es un evento que se registra cuando ocurre un problema, un fallo o un error graves en el funcionamiento de la aplicación o en la ejecución de un procedimiento.
- Una *advertencia* es un evento al que se debe atender porque destaca una situación importante en el funcionamiento de Kaspersky Thin Client y puede anticipar un problema futuro. La mayoría de los eventos se catalogan como advertencias si, a pesar de que el evento haya ocurrido, la aplicación puede recuperarse sin sufrir una pérdida de información o de funcionalidad.
- Un evento *Información* es un evento que se registra para informar que una operación o procedimiento se completaron sin errores o que la aplicación funciona correctamente.

Puede utilizar Kaspersky Security Center Web Console para configurar notificaciones sobre los eventos de Kaspersky Thin Client para un dispositivo o para un grupo de dispositivos.

Cómo configurar las notificaciones de eventos para un dispositivo

1. En la ventana principal de Kaspersky Security Center Web Console, realice una de las siguientes acciones:

- Si el cliente ligero está incluido en un grupo de administración, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
- Si el cliente ligero no forma parte de ningún grupo de administración, seleccione **Descubrimiento y despliegue** → **Dispositivos no asignados**.

2. Haga clic en el nombre del dispositivo con Kaspersky Thin Client. Encontrará el nombre del dispositivo [en la interfaz de Kaspersky Thin Client](#).

3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.

4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.

Se abre una ventana con información sobre Kaspersky Thin Client.

5. Seleccione la pestaña **Configuración de eventos**.

6. Seleccione la importancia de los eventos cuya información desee recibir:

- **Crítico**
- **Error funcional**
- **Advertencia**
- **Información**

Aparece una tabla de eventos asociados al nivel de importancia seleccionado.

7. Haga clic en el botón **Agregar evento** y, en la ventana que se abre, marque las casillas ubicadas junto a los tipos de eventos que desee agregar.

8. Haga clic en **Aceptar**.

9. Para guardar los cambios, haga clic en el botón **Guardar**.

Kaspersky Thin Client enviará los tipos de eventos seleccionados con la importancia especificada al Servidor de administración de Kaspersky Security Center. De manera predeterminada, los eventos se almacenan por treinta días.

Cómo configurar notificaciones de la configuración de eventos para los dispositivos que estén dentro de un grupo de administración

1. En la ventana principal de Web Console, seleccione **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva del complemento web Kaspersky Security Management Suite.

3. En la ventana que se abre, seleccione la pestaña **Configuración de eventos**.

4. Seleccione la importancia de los eventos cuya información desee recibir:

- **Crítico**
- **Error funcional**
- **Advertencia**
- **Información**

Aparece una tabla de eventos asociados al nivel de importancia seleccionado.

5. Haga clic en el botón **Agregar evento** y, en la ventana que se abre, marque las casillas ubicadas junto a los tipos de eventos que desee agregar.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios, haga clic en el botón **Guardar**.

Si el interruptor **Imponer** está desactivado, los ajustes no se aplicarán a los dispositivos con Kaspersky Thin Client que formen parte del grupo de administración y estén sujetos a la directiva de seguridad vigente.

Kaspersky Thin Client enviará los tipos de eventos seleccionados con la importancia especificada al Servidor de administración de Kaspersky Security Center. De manera predeterminada, los eventos se almacenan por treinta días.

Para obtener información detallada sobre cómo configurar las notificaciones sobre el registro de eventos en Kaspersky Security Center Web Console, consulte la [Ayuda en línea de Kaspersky Security Center](#).

Ver los eventos de Kaspersky Thin Client en Web Console

Puede ver los eventos registrados por Kaspersky Thin Client en Web Console.

Para ver los eventos registrados por Kaspersky Thin Client en Web Console:

1. En la ventana principal de Kaspersky Security Center Web Console, realice una de las siguientes acciones:

- Si el cliente ligero está incluido en un grupo de administración, seleccione **Activos (dispositivos)** → **Dispositivos administrados**.
- Si el cliente ligero no forma parte de ningún grupo de administración, seleccione **Descubrimiento y despliegue** → **Dispositivos no asignados**.

2. Haga clic en el nombre del dispositivo pertinente. Encontrará el nombre del dispositivo en la [interfaz de Kaspersky Thin Client](#).

3. En la ventana que se abre, seleccione la pestaña **Eventos**.

Se abre una ventana con una tabla de eventos registrados. Para cada evento, se brinda la siguiente información:

- **Hora:** muestra la fecha y la hora en que Web Console recibió el evento registrado por Kaspersky Thin Client.
- **Evento:** muestra el tipo de evento.
- **Descripción:** muestra una breve descripción del evento registrado.
- **Aplicación:** muestra el nombre de la aplicación a la cual corresponde el evento recibido en Web Console.
- **Número de versión:** muestra la versión de la aplicación correspondiente al evento recibido en Web Console.
- **El nivel de importancia** muestra la gravedad del evento.
- **Tarea:** muestra el nombre de la tarea que se ejecutará cuando se registre el evento.
- **Registrado:** muestra la fecha y la hora en que el evento se registró en el dispositivo.

Solución de problemas

Ante un error, verifique lo siguiente:

1. [Que el cliente ligero esté encendido.](#)
2. [Que el cliente ligero esté conectado a la red.](#)
3. [Que no haya errores en la dirección IP \(o el nombre del servidor\), el nombre de usuario y la contraseña que se ingresaron al conectarse al entorno remoto.](#)

Si no puede resolver el problema, comuníquese con [Soporte técnico](#). Si es necesario, los expertos de Soporte técnico pueden pedirle que proporcione información del sistema o [registros de eventos y de auditoría](#).

Restablecer una conexión remota tras una desconexión

Si se interrumpe la conexión entre Kaspersky Thin Client y el entorno remoto, se intentará restablecer la conexión automáticamente en tanto esta función se haya activado en los ajustes de la conexión remota.

Si no se logra restablecer la conexión en el intento de reconexión o si la opción de reconexión automática no está habilitada, la pantalla de la sesión remota se cierra y aparece un mensaje con el motivo del error.

Para reanudar la sesión remota:

1. Cierre el mensaje de error.
2. Intente conectarse al entorno remoto.
3. Si aún no puede conectarse, solicite ayuda a su administrador: podría haber un problema en la red física que impida la conexión entre Kaspersky Thin Client y el escritorio remoto.
4. Si se establece la conexión directa, pero aún no puede conectarse al escritorio remoto, comuníquese con [Soporte técnico](#).

Problemas al restringir el acceso a las funciones del complemento web de Kaspersky Security Management Suite

Después de [instalar](#) o [actualizar](#) el complemento web de Kaspersky Security Management Suite, es posible que [los usuarios con un conjunto completo de derechos](#) no tengan acceso a algunas funciones de la aplicación.

Para solucionar los problemas con el acceso compartido a las funciones del complemento web:

1. Coloque el archivo RBAC del [kit de distribución del complemento web](#) en los siguientes directorios del [Servidor de administración](#):

a. <Directorio de instalación de Kaspersky Security Center>/rbac

b. /var/opt/kaspersky/klnagent_srv/1093/dat/rbac

2. Reinicie el Servidor de administración.

Los usuarios deben tener derecho de acceso a las funciones del complemento Web Access de acuerdo con sus roles.

Si no puede resolver el problema, comuníquese con el [Servicio de soporte técnico](#).

Comunicarse con Soporte técnico

Si tiene problemas [que no puede resolver por su cuenta](#) al utilizar Kaspersky Thin Client, comuníquese con [Soporte técnico de Kaspersky](#).

Antes de comunicarse con Soporte técnico, asegúrese de leer las [reglas de soporte técnico](#).

Cuando se comunique con Soporte técnico, nuestros especialistas podrían pedirle sus [registros de eventos y de auditoría](#). Puede utilizar la interfaz de Kaspersky Thin Client para [enviar estos registros a un servidor de registros](#) instalado en la infraestructura de su organización, desde el cual los especialistas podrán descargarlos.

Acerca de los registros de Kaspersky Thin Client

Kaspersky Thin Client mantiene dos tipos de registros:

- Registro de eventos. Aquí se almacenan todos los [eventos](#) registrados por los componentes de Kaspersky Thin Client. Puede ver el registro de eventos en la interfaz de Kaspersky Thin Client. También puede [enviarlo a un servidor de registros](#).
- Registro de auditoría. Este registro almacena eventos importantes del funcionamiento del cliente ligero, como la interacción con los certificados para conectarse a Kaspersky Security Center, la información sobre el Servidor de administración y las conexiones o desconexiones del mismo, y los restablecimientos de fábrica del dispositivo. El registro de auditoría no puede consultarse mediante la interfaz de Kaspersky Thin Client. Puede [enviar el archivo del registro de auditoría a un servidor de registros](#).

Registro de eventos

El registro de eventos de Kaspersky Thin Client contiene la siguiente información:

- Fecha y hora en que ocurrió un evento.
- Nombre del componente de Kaspersky Thin Client que registró el evento.
- Gravedad del evento. Los valores posibles son los siguientes:
 - *Trace*. Comprende todos los mensajes y advertencias que pueden surgir durante el funcionamiento de la aplicación.
 - *Debug*. Comprende los mensajes de depuración, los mensajes informativos e importantes y todas las advertencias y mensajes sobre errores críticos y comunes.
 - *Info*. Comprende los mensajes informativos, los mensajes importantes y todas las advertencias y mensajes sobre errores críticos y comunes.
 - *Warn*. Comprende todas las advertencias y mensajes sobre errores críticos y comunes.
 - *Error*. Comprende los mensajes sobre errores y errores críticos en el funcionamiento de la aplicación.
 - *Fatal*. Comprende los mensajes sobre errores críticos en el funcionamiento de la aplicación.

- Información de depuración en formato <Archivo>:<Número de línea>,<Función>, donde:
 - *File* es un nombre de archivo.
 - *Line Number* es un número de línea dentro del archivo.
 - *Function* es información de depuración.
- Id. de proceso e id. de subprocesso.
- Id. de la versión del producto.

Registro de auditoría

El registro de auditoría de Kaspersky Thin Client contiene la siguiente información:

- Agregar, reemplazar y cambiar certificados para conectarse a Kaspersky Security Center en la interfaz de Kaspersky Thin Client:
 - Fecha y hora del evento.
 - Dirección IP y/o nombre de dominio del Servidor de administración de Kaspersky Security Center.
 - Número de puerto del Servidor de administración de Kaspersky Security Center.
 - Id. del cliente ligero.
 - Lista de atributos del certificado: nombre del emisor, nombre del sujeto, huella digital del certificado, fecha y hora de inicio de validez, fecha y hora de fin de validez.
- Habilitar (manual y automáticamente) y deshabilitar la administración de Kaspersky Thin Client a través de Kaspersky Security Center:
 - Fecha y hora del evento.
 - Dirección IP y/o nombre de dominio del Servidor de administración de Kaspersky Security Center.
 - Número de puerto del Servidor de administración de Kaspersky Security Center.
 - Id. del cliente ligero.
- Restablecimiento de los ajustes de Kaspersky Thin Client:
 - Fecha y hora del evento.
 - Id. del cliente ligero.
- Aceptar una conexión remota al cliente ligero:
 - Fecha y hora del evento.
 - Dirección IP y/o nombre de dominio del usuario que se conectó al cliente ligero.
 - Nombre del usuario que se conectó al cliente ligero.

- Crear un nuevo archivo de registro de auditoría en caso de rotación de registros:
 - Fecha y hora del evento.
 - Id. del cliente ligero.
 - Número de versión de Kaspersky Thin Client.
- Guardar y eliminar la contraseña de usuario para la conexión automática a un entorno remoto:
 - Fecha y hora del evento.
 - Nombre de usuario para conectarse al entorno remoto.

Enviar los registros a un servidor

Si se [comunica con Soporte técnico](#), puede que los especialistas de Kaspersky le soliciten sus [registros de eventos y de auditoría](#). Puede utilizar la interfaz de Kaspersky Thin Client para enviar estos registros a un servidor de registros, desde el cual los especialistas podrán descargarlos.

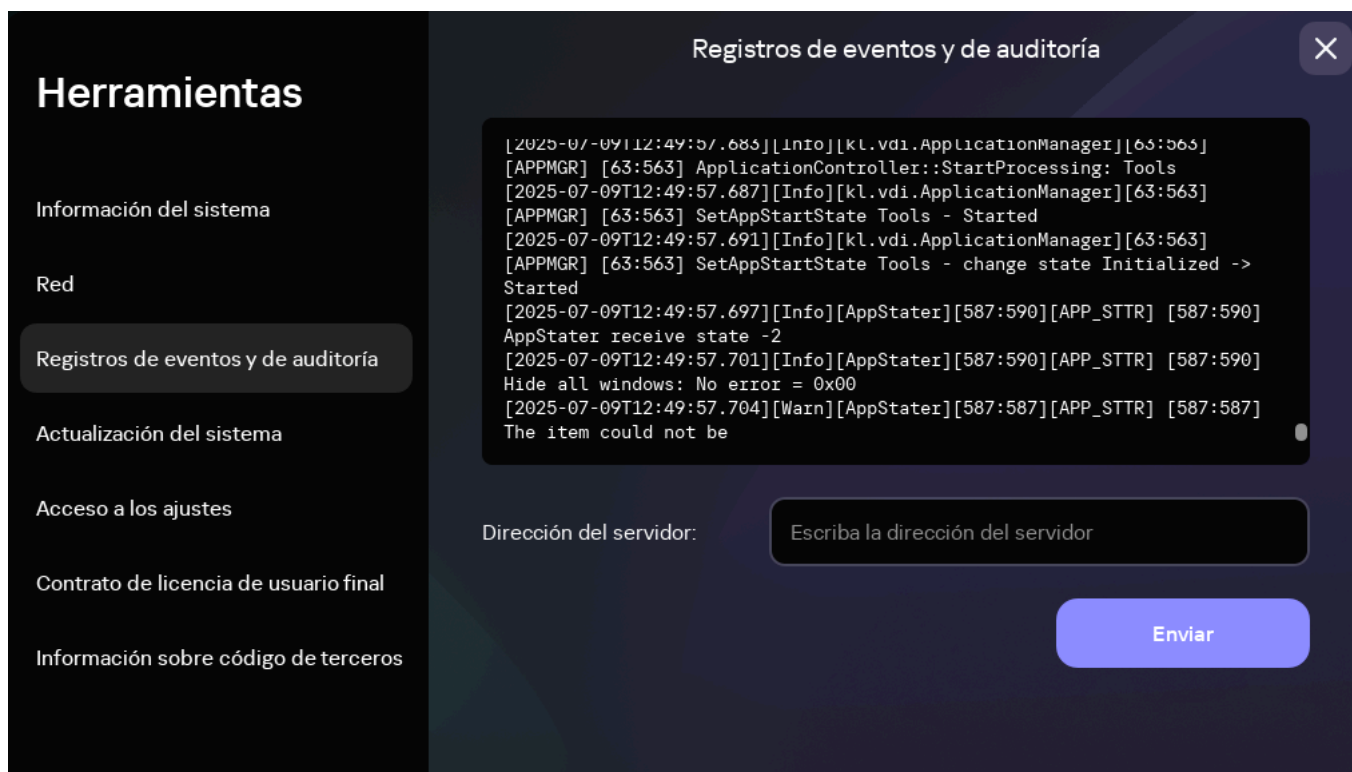
Como primera medida, asegúrese de contar con un [servidor de registros](#) instalado en la infraestructura de su organización. Para obtener información detallada sobre cómo instalar un servidor de registros, consulte la guía del administrador de dicho servidor.

El tamaño de archivo máximo para el registro de eventos y el registro de auditoría es de 150 MB y 512 MB, respectivamente. Cuando el registro de eventos o el registro de auditoría alcanza su respectivo límite de tamaño, Kaspersky Thin Client elimina los registros existentes y comienza a guardar registrar nuevos. Cada vez que se actualizan los registros de eventos y de auditoría, se graba la versión instalada de Kaspersky Thin Client al comienzo del registro.

Para enviar los registros de eventos y de auditoría de Kaspersky Thin Client a un servidor de registros:

1. En el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Herramientas**.
2. En la ventana que se abre, elija la sección **Registros de eventos y de auditoría** (vea la siguiente imagen).

Esta sección muestra las entradas del registro de eventos. Las entradas del registro de auditoría no se muestran en la interfaz de Kaspersky Thin Client.



Herramientas. Sección Registros de eventos y de auditoría

Aparecerá información sobre los eventos registrados en Kaspersky Thin Client.

3. En el campo **Dirección del servidor**, ingrese la dirección del servidor que recibirá los registros de auditoría y de eventos. A continuación, haga clic en el botón **Enviar**.

Si el cliente ligero pertenece a un [grupo de administración](#), la dirección del servidor de registros se puede [imponer a través de la Consola web](#). En este caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

Recomendamos verificar que no haya errores en la dirección del servidor de destino al que se vayan a enviar los registros. Si ingresa la dirección incorrecta, los registros podrían quedar expuestos a terceros.

4. En la ventana que se abre, confirme que desea enviar los registros de eventos y de auditoría.

Si el dispositivo no es miembro de un [grupo de administración](#) y esta es la primera vez que envía registros de eventos y de auditoría al servidor de registros, verá una ventana que le pedirá que agregue un [certificado para conectarse al servidor de registros](#).

Verifique la configuración del certificado que está agregando y haga clic en el botón **Agregar certificado**. El certificado se agregará al almacén de certificados del sistema de Kaspersky Thin Client y se usará en las subsiguientes conexiones.

Los registros de eventos y de auditoría de Kaspersky Thin Client se reenviarán al servidor especificado.

Glosario

Administrador de Kaspersky Security Center

Persona que administra las operaciones del cliente ligero a través del sistema de administración remota y centralizada conocido como Kaspersky Security Center.

Agente

Servicio que controla el acceso y las conexiones a aplicaciones y escritorios remotos (un ejemplo es el Agente de conexión a Escritorio remoto de Microsoft).

Aplicación virtual

Aplicación que se encuentra instalada en un servidor remoto. Para conectarse a una aplicación virtual, se deben usar tecnologías de acceso remoto.

Cliente ligero

Computadora personal compacta usada para conectarse a través de una red a servidores remotos que permiten almacenar información y que tienen instaladas todas las aplicaciones necesarias para trabajar. El cliente ligero lleva conectados diferentes periféricos, como un monitor, un teclado y un mouse.

Complemento web Kaspersky Security Management Suite

Componente especializado que brinda una interfaz para administrar los ajustes de Kaspersky Thin Client a través de la Consola de administración de Kaspersky Security Center.

Directiva

Una directiva determina los ajustes de Kaspersky Thin Client y define el acceso a los ajustes de sistema de Kaspersky Thin Client en los dispositivos pertenecientes a un grupo de administración. Puede crear un número ilimitado de directivas para los dispositivos con Kaspersky Thin Client de cada grupo de administración, pero solamente puede haber una directiva aplicada a cada dispositivo con Kaspersky Thin Client dentro de cada grupo de administración.

Entorno remoto

Cualquier recurso remoto compatible, como un escritorio remoto o una aplicación virtual, al que el usuario de un cliente ligero pueda acceder mediante una tecnología de acceso remoto para trabajar.

Escritorio remoto

Sistema operativo que se encuentra instalado en una computadora o en un entorno virtual. Para conectarse a este tipo de sistema operativo, se deben utilizar tecnologías de acceso remoto.

Evento

Entrada que contiene registros de los cambios realizados en el estado o en la configuración de un cliente ligero o registros de errores que requieren la atención de un administrador del sistema.

Grupo de administración

Conjunto de dispositivos administrados por Kaspersky Security Center y agrupados por función. Agrupar los dispositivos ayuda a administrarlos en forma conjunta. Un grupo puede incluir otros grupos. Para cada dispositivo agregado al grupo, puede crear directivas de grupo y tareas de grupo aplicables a todos los dispositivos del grupo.

Servidor de administración

Componente de la aplicación Kaspersky Security Center que permite almacenar y administrar centralmente información sobre las aplicaciones de Kaspersky instaladas en la red de una empresa.

Servidor de registros

Servidor que recibirá [los registros de eventos y de auditoría](#) de Kaspersky Thin Client. Este servidor debe estar instalado en la red corporativa.

Sesión remota

Sesión de trabajo en el entorno remoto al que el usuario se ha conectado a través de la interfaz del cliente ligero.

TLS

Protocolo seguro que utiliza cifrado para transferir datos en redes locales y en Internet.

Información sobre código de terceros

Encontrará información sobre código de terceros en el archivo `LegalNotices_en.txt` que forma parte del kit de distribución.

También puede ver información sobre código de terceros en la interfaz de Kaspersky Thin Client.

Para ver información sobre código de terceros,

en el panel de control de Kaspersky Thin Client, haga clic en  y, en el menú que se abre, seleccione **Herramientas → Información sobre código de terceros**.

Se abre una ventana con información sobre el uso de código de terceros en la versión de Kaspersky Thin Client instalada.

Avisos de marcas comerciales

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

Ubuntu es una marca registrada de Canonical Ltd.

Citrix, Citrix Workspace son marcas registradas o marcas de Cloud Software Group, Inc. o sus subsidiarias en los Estados Unidos o en otros países.

Dell y otras marcas son marcas comerciales de Dell Inc. o sus subsidiarias.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y en otros países.

Microsoft, RemoteFX, Windows y Windows Server son marcas comerciales del grupo de empresas Microsoft.

OpenSSL es una marca comercial propiedad de OpenSSL Software Foundation.

JavaScript es una marca registrada de Oracle y/o de sus empresas vinculadas.