kaspersky

Kaspersky Thin Client

© 2025 AO Kaspersky Lab

Contenido

Ayuda de Kaspersky Thin Client

<table>
<tr>
<td>  </td>
<td>Novedades
<a>Qué hay de nuevo en esta versión de Kaspersky Thin Client</td>
<td>  </td>
<td>Requisitos de hardware y software
<a>Requisitos para los entornos remotos y los periféricos conectados</td>
</tr>
<tr>
<td>  </td>
<td>Actualización
<a>Cómo actualizar la versión de Kaspersky Thin Client</td>
<td>  </td>
<td>Restablecimiento de ajustes y datos
<a>Cómo restablecer los ajustes y los datos de Kaspersky Thin Client</td>
</tr>
<tr>
<td>  </td>
<td>Primeros pasos
<a>Encender el cliente ligero
<a>Realizar la configuración inicial y conectarse a Kaspersky Security Center
<a>Asignar certificados</td>
<td>  </td>
<td>Configuración y conexión a un entorno remoto
<a>Opciones de conexión disponibles
<a>Conectarse a un entorno remoto
<a>Configurar los ajustes de Kaspersky Thin Client y los parámetros para conectarse a entornos remotos y a Kaspersky Security Center
<a>Configurar los clientes ligeros a través de Kaspersky Security Center</td>
</tr>
<tr>
<td>  </td>
<td>Funciones avanzadas
<a>Administrar los certificados de Kaspersky Thin Client
<a>Administrar directivas
<a>Configurar el acceso a los ajustes de Kaspersky Thin Client</td>
<td>  </td>
<td>Supervisión de eventos
<a>Ver los registros de eventos y de auditoría; enviar estos registros a un servidor de registros
<a>Ver los eventos de Kaspersky Thin Client a través de Kaspersky Security Center Web Console</td>
</tr>
</table>

Acerca de Kaspersky Thin Client

Kaspersky Thin Client versión 2.0 (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 versión 2.0 solo se puede instalar en clientes ligeros TONK TN1200 o Centerm F620.

Principales funciones de Kaspersky Thin Client:

- 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), con autorización mediante nombre de usuario y contraseña.
- 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), con autorización mediante nombre de usuario y contraseña.
- Conéctese a escritorios remotos y virtuales que ejecuten sistemas operativos Linux® a través del protocolo de escritorio remoto RDP, con autorización mediante nombre de usuario y contraseña.
- Conéctese a aplicaciones virtuales a través del protocolo RDP, utilizando el Agente de conexión a Escritorio remoto de Microsoft y con autorización mediante nombre de usuario y contraseña.
- Conéctese a escritorios virtuales implementados en una infraestructura de escritorios virtuales Basis.WorkPlace con autorización mediante nombre de usuario y contraseña.
- Conéctese a escritorios virtuales implementados en una infraestructura de Citrix Workspace o VMware Horizon a través de la aplicación Web Access.
- Transmita la pantalla del escritorio remoto al monitor conectado a Kaspersky Thin Client.
- Redireccione un teclado y un mouse conectados a Kaspersky Thin Client a un entorno remoto.
- Redireccione al entorno remoto las unidades de memoria USB, las tarjetas inteligentes, los tókenes USB, las impresoras, el micrófono y los dispositivos de reproducción de audio que conecte a Kaspersky Thin Client.
- Administre, actualice y supervise de manera centralizada Kaspersky Thin Client a través de Kaspersky Security Center Web Console versión 14.2. El complemento web Kaspersky Security Management Suite se utiliza para la comunicación entre Kaspersky Thin Client y Kaspersky Security Center.

Kit de distribución

Kaspersky Thin Client 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 preinstalado entregada por socios.

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

- Un archivo de almacenamiento con la imagen de instalación de Kaspersky Thin Client: Kaspersky_Thin_Client_<número de versión>.tar.gz.
- Un paquete de arranque: KTC_uboot_<número de versión>.tar.gz.
- Un script para realizar la instalación en el cliente ligero: hw_install.sh.
- Un archivo de texto con información sobre código de terceros: KTC_LegalNotices_en.txt.
- Archivos de texto que describen las nuevas funciones y las limitaciones conocidas:
  - ReleaseNotes_Kaspersky_Thin_Client_<número de versión>_EN.txt.
  - ReleaseNotes_Kaspersky_Thin_Client_<número de versión>_ES.txt.
  - ReleaseNotes_Kaspersky_Thin_Client_<número de versión>_PT_BR.txt.
  - ReleaseNotes_Kaspersky_Thin_Client_<número de versión>_RU.txt.
- Archivos del Contrato de licencia de usuario final de Kaspersky Thin Client:
  - eula_en_ktc_<número de versión>.txt.
  - eula_es_ktc_<número de versión>.txt.
  - eula_pt_ktc_<número de versión>.txt.
  - eula_ru_ktc_<número de versión>.txt.

El kit de distribución de Kaspersky Security Management Suite versión 2.0 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 Microsoft Windows que contienen las imágenes de instalación y los archivos de firma del complemento web para Kaspersky Security Center Web Console:
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número de versión del complemento>_en.exe.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número de versión del complemento>_es.exe.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número de versión del complemento>_pt_br.exe.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número de versión del complemento>_ru.exe.
- Archivos para Linux que contienen las imágenes de instalación y los archivos de firma del complemento web para Kaspersky Security Center Web Console:
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número de versión del complemento>_en.sh.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número de versión del complemento>_es.sh.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número de versión del complemento>_pt_br.sh.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número de versión del complemento>_ru.sh.
- Un archivo de texto con información sobre código de terceros para Kaspersky Security Management Suite: KSMS_LegalNotices_en.txt.
- Archivos del Contrato de licencia de usuario final de Kaspersky Security Management Suite:
  - eula_en_ksms_<número de versión>.txt.
  - eula_es_ksms_<número de versión>.txt.
  - eula_pt_ksms_<número de versión>.txt.
  - eula_ru_ksms_<número de versión>.txt.

Funcionamiento de Kaspersky Thin Client

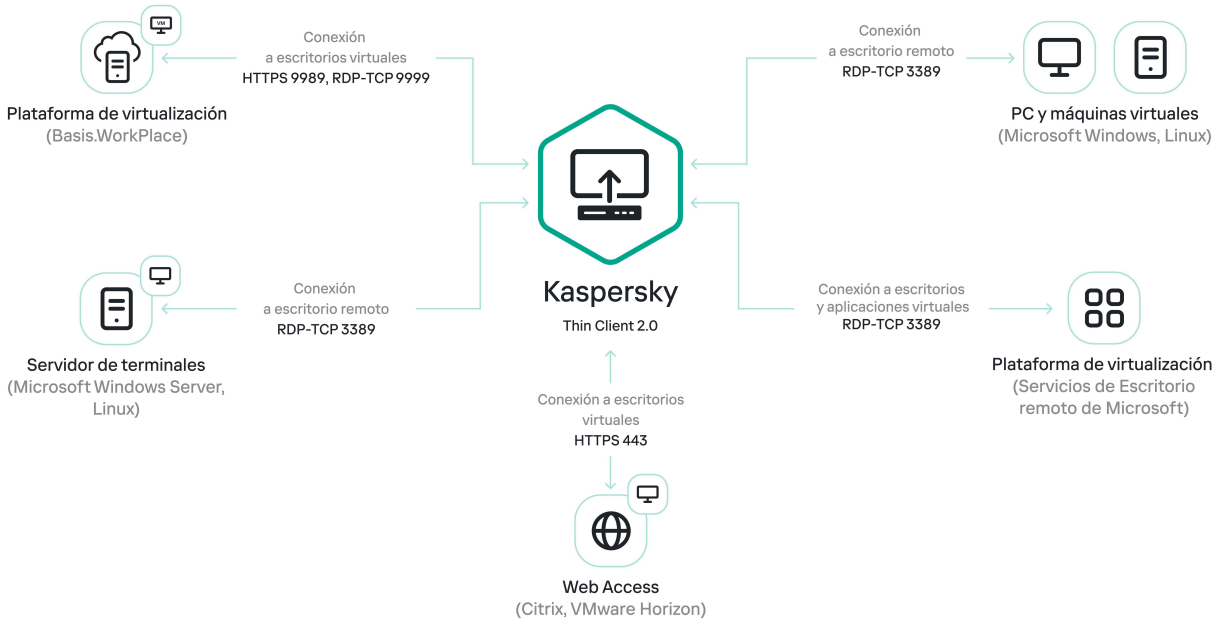
El esquema de funcionamiento estándar de Kaspersky Thin Client (representado en la imagen de más abajo) puede diagramarse de este modo:

- Una vez instalado en la plataforma de hardware adecuada, Kaspersky Thin Client obtiene sus ajustes de red de un servidor DHCP (o utiliza los ajustes de red definidos manualmente por el administrador).
- El administrador conecta Kaspersky Thin Client con Kaspersky Security Center y configura la interacción entre ambos.

- Kaspersky Thin Client recibe de Kaspersky Security Center los ajustes de conexión a un escritorio remoto o a una aplicación virtual (en adelante, también denominados "sesión de conexión") junto con actualizaciones, certificados de confianza, la fecha, la hora y la directiva.
- El usuario se conecta al escritorio remoto o a la aplicación virtual a través de RDP.
- El usuario se conecta al escritorio remoto a través de la plataforma de virtualización Basis.WorkPlace.
- El usuario se conecta al entorno remoto en Web Access.
- En la interfaz de Kaspersky Thin Client, el usuario envía registros de eventos y registros de auditoría a un servidor de registros.
- Kaspersky Thin Client utiliza Kaspersky Security Center para recibir actualizaciones de software del servidor de actualización de Kaspersky.

Esquema de funcionamiento estándar de Kaspersky Thin Client

La siguiente imagen muestra el diagrama de comunicación entre Kaspersky Thin Client y las plataformas de virtualización.



Comunicación entre Kaspersky Thin Client y las plataformas de virtualización

Requisitos de hardware y software

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

Requisitos para los monitores conectados a Kaspersky Thin Client

Kaspersky Thin Client permite conectar dos monitores.

Kaspersky Thin Client admite las siguientes resoluciones de monitor:

- 1024 × 768
- 1280 × 800
- 1280 × 1024
- 1366 × 768
- 1440 × 900
- 1600 × 900
- 1680 × 1050

- 1920 × 1080
- 1920 × 1200. Si se conecta un monitor con esta resolución, la resolución real estará limitada a 1920 × 1080.

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:

- Teclado con cable y ratones estándar sin funcionalidad multimedia conectados a través de puertos USB.
- Unidades de memoria USB y tarjetas inteligentes o tokens que se conecten a través de puertos USB.
- Impresoras que se conecten a través de puertos USB. El entorno remoto debe tener instalado el controlador de la impresora conectada al cliente ligero.
- Dispositivos de grabación y reproducción de audio con cable, que se conecten a través de una miniclavija.

Requisitos para escritorios remotos

Puede conectarse a computadoras remotas, máquinas virtuales y servidores de terminales que tengan instalado uno de los siguientes sistemas operativos:

- Microsoft Windows 7
- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Astra Linux Common Edition 2.12 (xRDP 0.9.21.1)
- Astra Linux Special Edition 1.7 (xRDP 0.9.21.1)
- ALT Linux 10 (xRDP 0.9.24)
- RED OS® 7.3 (xRDP 0.9.23.1)

Requisitos para escritorios remotos de Basis.WorkPlace

Kaspersky Thin Client puede interactuar con la plataforma de virtualización Basis.WorkPlace versión 1.96. Puede utilizar el agente de Basis.WorkPlace para conectarse a escritorios remotos que ejecuten uno de los siguientes sistemas operativos:

- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Astra Linux Common Edition 2.12 (xRDP 0.9.21.1)
- Astra Linux Special Edition 1.7 (xRDP 0.9.21.1)
- ALT Linux 10 (xRDP 0.9.24)
- RED OS 7.3 (xRDP 0.9.23.1)

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 14.2 de Kaspersky Security Center. 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 los servidores de registros de eventos

El servidor de registros al que se remiten los registros de eventos y de auditoría de Kaspersky Thin Client es instalado en la infraestructura de la empresa por los especialistas de dicha empresa.

El servidor de registros tiene 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 de destino utilizando el método PUT.

Métodos de conexión remota

En esta sección, se describen los entornos y las tecnologías de acceso remoto que son compatibles con Kaspersky Thin Client, así como los métodos que se pueden utilizar para conectarse a esos entornos. También se brinda información sobre los dispositivos conectados a Kaspersky Thin Client que se pueden redireccionar a los entornos remotos.

Conexión mediante 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.

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.

Antes de conectarse a un escritorio remoto Linux a través de un servidor xRDP para el que no se haya instalado la extensión Kaspersky USB Redirector, verifique qué versión de servidor xRDP es compatible en el artículo correspondiente.

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 7	Windows 10/11	Windows Server 2016/2019/2022	ALT Linux 10 Red OS 7.3 Astra Linux CE 2.12	Astra Linux SE 1.7
Conexión a una aplicación virtual	✓	—	✓ Nota	✓	—	—
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	—
Micrófono (miniclavija)	✓	—	✓	✓ Nota	✓ Nota	✓ Nota
Dispositivo de reproducción de audio	✓	✓	✓	✓	✓ Nota	✓ Nota

Conexión mediante 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.

Antes de conectarse a un escritorio remoto Linux a través de un servidor xRDP para el que no se haya instalado la extensión Kaspersky USB Redirector, verifique qué versión de servidor xRDP es compatible en el artículo correspondiente.

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 7.3 ALT Linux 10 Astra Linux CE 2.12 Astra Linux SE 1.7
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	—
Micrófono (miniclavija)	✓	✓	✓
Dispositivo de reproducción de audio	✓	✓	✓

Conexiones con la aplicación Web Access

En la aplicación Web Access, puede conectarse a un entorno remoto desplegado en infraestructuras Citrix Workspace y VMware Horizon. 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.

Si desea obtener instrucciones para establecer una 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	—	✓
Periféricos		
Tokens USB	—	—
Tarjetas inteligentes (USB)	—	—
Unidades de memoria USB	—	—
Impresoras (USB)	—	—
Micrófono (miniclavija)	✓	✓
Dispositivo de reproducción de audio	✓	✓

En la versión actual de Kaspersky Thin Client, la aplicación Web Access no permite conectarse a aplicaciones virtuales ni a escritorios remotos que ejecuten Linux.

Novedades

Kaspersky Thin Client versión 2.0 ofrece las siguientes mejoras y características nuevas:

- Conexión a escritorios remotos y aplicaciones desplegados en una infraestructura de Servicios de Escritorio remoto de Microsoft: ahora puede iniciar sesión en aplicaciones virtuales y escritorios Microsoft Windows remotos a través del Agente de conexión a Escritorio remoto de Microsoft.
- A partir de ahora, puede utilizar HTML5 para conectarse a escritorios virtuales desplegados en infraestructuras Citrix Workspace y VMware Horizon.
- Redirección al entorno remoto de los dispositivos de grabación y reproducción de audio conectados al cliente ligero mediante un conector con miniclavija.
- Redirección de impresoras, tarjetas inteligentes y unidades de memoria USB a escritorios remotos que ejecuten Linux (Astra Linux CE/SE, ALT Linux o RED OS). Para redireccionar periféricos, se debe instalar Kaspersky USB Redirector para el servidor xRDP en el sistema operativo invitado (incluido el sistema operativo invitado que haya instalado en Basis.WorkPlace).
- Ahora es compatible con el cliente ligero Centerm F620.
- Conexión automática tras una desconexión inesperada: se agregó la capacidad de conectarse automáticamente a un escritorio remoto a través de RDP si se interrumpe la conexión.
- Ampliaciones en la compatibilidad con sistemas operativos invitados: a partir de esta versión, puede conectarse a escritorios remotos que ejecuten Microsoft Windows 11 y Microsoft Windows Server 2022.
- Redirección de impresoras al entorno remoto: ahora puede utilizar una impresora conectada al cliente ligero para imprimir documentos desde el sistema operativo invitado (función disponible para conexiones establecidas a través de RDP, incluso en infraestructuras de escritorios virtuales de Basis.WorkPlace).
- Compatibilidad con una nueva configuración de TONK TN1200: a partir de ahora, puede iniciar y utilizar Kaspersky Thin Client en dispositivos TONK TN1200 que cuenten con un disco de estado sólido mSATA.
- Mejoras en el rendimiento de Kaspersky Thin Client:
  - El escritorio remoto y las aplicaciones virtuales ahora llegan al cliente ligero con mayor velocidad.
  - Se redujo el tiempo de arranque de los clientes ligeros.
  - Se aumentó la velocidad para conectarse a escritorios remotos por nombre de dominio.
- Se mejoró la estabilidad de los clientes ligeros administrados a través de Kaspersky Security Center.
- El español y el portugués de Brasil ahora están disponibles como idiomas de entrada e interfaz de usuario.
- Se actualizaron el diseño y el texto de la interfaz de usuario de Kaspersky Thin Client:
  - Se rediseñó el panel de conexión del entorno remoto.
  - Se agregó un panel de notificaciones interactivo.

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.

Preparativos para la instalación

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:
   - KTC_uboot_<número de versión>.tar.gz: paquete de arranque.
   - Kaspersky_Thin_Client_<número de versión>.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.

Instalar Kaspersky Thin Client

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 utilizando una cuenta con privilegios de root:

   ```
   sudo ./hw_install.sh -b KTC_uboot_<número de versión>.tar.gz -u
   Kaspersky_Thin_Client_<número de versión>.tar.gz
   ```

   donde:

   - `./hw_install.sh`: ruta al script de instalación.
   - `KTC_uboot_<número de versión>.tar.gz`: paquete de arranque.
   - `Kaspersky_Thin_Client_<número de versión>.tar.gz`: imagen de instalación.

   Si la instalación concluye sin errores, aparecerá el mensaje *Installed OK! Remove USB drive and reboot* ("Instalado correctamente. Desconecte la unidad USB y reinicie").

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

Para actualizar Kaspersky Thin Client a la versión 2.0, debe obtener de los especialistas de Kaspersky un archivo que contenga actualizaciones para las bases de datos. Cargue este archivo en Kaspersky Security Center Web Console (en adelante, también denominado "Web Console") y luego, mediante la interfaz de Web Console, cree, configure y ejecute una tarea para descargar actualizaciones en el repositorio del Servidor de administración de Kaspersky Security Center (en adelante, también denominado "Servidor").

Para actualizar Kaspersky Thin Client, el cliente ligero debe estar conectado a Kaspersky Security Center.

Cada Servidor de administración de Kaspersky Security Center puede tener una única tarea de actualización activa, con un único origen de actualizaciones prioritario. Por ello, recomendamos que utilice un Servidor independiente para administrar los clientes ligeros; esto le permitirá seguir recibiendo los parches de seguridad críticos de los servidores de actualización de Kaspersky.

Para actualizar Kaspersky Thin Client en el cliente ligero mediante Kaspersky Security Center Web Console:

1. En el Servidor de Kaspersky Security Center, descomprima el archivo con las actualizaciones para las bases de datos que le hayan brindado los especialistas de Kaspersky.

2. Otorgue a todos los usuarios del sistema derechos de acceso completo a la carpeta descomprimida realizando las siguientes acciones:

   a. Haga clic con el botón derecho en la carpeta descomprimida y seleccione **Propiedades**.

   b. En el menú que se abre, seleccione la ficha **Seguridad** y haga clic en **Editar**.

   c. En la ventana que se abre, haga clic en **Agregar**, luego seleccione **Avanzado** y, en la ventana que se abre, haga clic en **Buscar ahora**.

   d. En la lista que aparece, seleccione el grupo **Todos** y haga clic en **Aceptar**, luego haga clic en **Aceptar** una vez más en la ventana que se abre.

      Aparece la ficha **Seguridad** y el grupo **Todos** aparece en la lista **Nombres de grupos o usuarios**.

   e. En la sección **Permisos para Todos**, seleccione las casillas de todos los parámetros en la columna **Permitir**.

   f. Haga clic en **Aceptar** y luego haga clic en **Aceptar** una vez más en la ventana que se abre.

3. Inicie Web Console y seleccione la sección **Dispositivos**, luego vaya a la pestaña **Tareas**.

4. Si la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** está disponible en la lista, continúe con el siguiente paso de las instrucciones. Si la tarea no está disponible, haga lo siguiente para agregarla:

   a. En la pestaña **Tareas**, haga clic en **Agregar**.

   b. En la ventana que se abre, en la lista desplegable **Tipo de tarea**, seleccione **Descargar actualizaciones en el repositorio del Servidor de administración** y haga clic en **Siguiente**.

   c. Haga clic en **Finalizar** para completar la creación de la tarea.

5. Seleccione la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** y, en la ventana que se abre, vaya a la pestaña **Configuración de la aplicación**.

6. En el grupo de configuración **Orígenes de actualizaciones**, seleccione la casilla junto al origen de los **Servidores de actualizaciones de Kaspersky** y haga clic en **Eliminar**.

7. En el mismo grupo de ajustes, haga clic en **Agregar** y luego, en la lista que aparece, seleccione **Carpeta local o de red** y especifique la ruta completa a la carpeta que contiene los archivos de actualización.

8. Haga clic en **Guardar** para completar el cambio del origen de actualizaciones.

9. Vaya a la pestaña **Programación** y seleccione el valor necesario en la lista desplegable **Inicio programado**.

   Configure los demás ajustes de la pestaña según sea necesario.

10. Haga clic en **Guardar** para completar la configuración de la tarea.

11. En la lista de tareas, seleccione la casilla junto a la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** y haga clic en **Iniciar**.

    Se inicia la ejecución de la tarea. Puede realizar un seguimiento del progreso de la tarea en la lista de tareas, en la columna **Estado**.

12. Para ver el resultado de una tarea para dispositivos individuales:

    a. En la lista de tareas, seleccione **Descargar actualizaciones en el repositorio del Servidor de administración** y, en la ventana que se abre, vaya a la pestaña **Resultados**.

    b. Para ver información detallada sobre la ejecución de la tarea en un dispositivo, seleccione la casilla junto al dispositivo requerido y haga clic en **Historial del dispositivo**.

13. Una vez finalizada la tarea de descarga de actualizaciones, siga los siguientes pasos para aceptar el Contrato de licencia de usuario final y aprobar la descarga de actualizaciones a los clientes ligeros:

    a. En Web Console, vaya a **Operaciones** → **Aplicaciones de Kaspersky** y seleccione **Actualizaciones sin interrupciones** en la lista desplegable.

    b. En la lista de actualizaciones que aparece, haga clic en **Debe aceptar el Contrato de licencia de usuario final (EULA)** junto a la actualización requerida y, en la ventana que se abre, lea el texto del Contrato de licencia de usuario final.

    c. Si está de acuerdo con los términos del acuerdo, acéptelo seleccionando la casilla **Los términos y las condiciones de este EULA** y confirmando su elección. Si no está de acuerdo con los términos del Contrato de licencia de usuario final y no los acepta, no podrá descargar actualizaciones para clientes ligeros.

    d. En la lista de actualizaciones, haga clic en el nombre de la actualización y, en la sección **Estado de aprobación de la actualización** que aparece, seleccione **Aprobada** y confirme su elección.

    Para obtener información detallada sobre la aprobación de descargas de actualizaciones, consulte *Aprobar y rechazar actualizaciones de software* en la Ayuda en línea de Kaspersky Security Center.

    Se aprobará la solicitud de descarga de la actualización.

Una vez aprobada la solicitud, las actualizaciones se descargan en los clientes ligeros conectados a Kaspersky Security Center, incluso en los que no forman parte de los grupos de administración o los grupos de dispositivos administrados.

La información detallada sobre cómo recibir e instalar actualizaciones en clientes ligeros se proporciona en un artículo aparte.

Interfaz de Kaspersky Thin Client

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

- Ventana principal de Kaspersky Thin Client.

  En la parte central de la ventana principal, puede seleccionar una opción de conexión remota:

  - **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 o VMware Horizon.

  En la ventana de conexión, puede configurar los ajustes de la conexión RDP o los ajustes de la conexión a Basis.WorkPlace.

- Panel de control de Kaspersky Thin Client. Contiene los siguientes elementos:

  - : botón del menú de apagado. Utilice este menú para apagar o reiniciar Kaspersky Thin Client.
  - : 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.
    - Actualizar Kaspersky Thin Client.
    - Ver el Contrato de licencia de usuario final actual.
    - Ver información sobre el código de terceros.
    - Configurar el acceso a los ajustes de Kaspersky Thin Client.

  - Si Kaspersky Thin Client es miembro de un grupo de administración y se han agregado los datos de contacto del administrador en los ajustes generales del grupo, el panel de control también muestra la información de contacto del administrador de Kaspersky Security Center.
  - Estado de la conexión de red de Kaspersky Thin Client.
  - Información sobre nuevas notificaciones de Kaspersky Thin Client. Puede ver las notificaciones recibidas.
  - Botón para cambiar el idioma de entrada del teclado.
  - Fecha y hora del sistema.

- Panel de conexión.

  Aparece cuando hay una conexión activa a un entorno remoto.

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

- Nombre de la conexión.
- Estado de la conexión.
- Botón **Desconectarse del servidor**.
- Los contactos del administrador, siempre y cuando se los haya indicado al implementar el sistema.
- Icono de estado de la red.

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

- Icono de la aplicación.
- Fecha actual configurada en el cliente ligero.
- Hora actual configurada en el cliente ligero.
- Idioma configurado en el cliente ligero.

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:

- 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 con datos sobre los certificados cargados en Kaspersky Thin Client e información sobre los casos en los que se habilitó y deshabilitó la administración de los clientes ligeros a través de Kaspersky Security Center.
- Ajustes del cliente ligero:
  - 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.
  - Monitores principal y secundario.
  - Id. del monitor principal.
  - 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.

- 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.
  - Periodo 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 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, incluidas las 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.

- 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 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 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.
- 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 y apagar Kaspersky Thin Client

Antes de utilizar Kaspersky Thin Client, conecte un mouse, un teclado y un monitor al cliente ligero a través de los puertos correspondientes ubicados en el panel trasero del dispositivo. Para comenzar a trabajar con Kaspersky Thin Client, encienda el cliente ligero.

Kaspersky Thin Client permite conectar el mouse, el teclado y el monitor al cliente ligero mientras el sistema está en funcionamiento. Cuando se conecta un segundo monitor, se le pide que configure el formato del monitor.

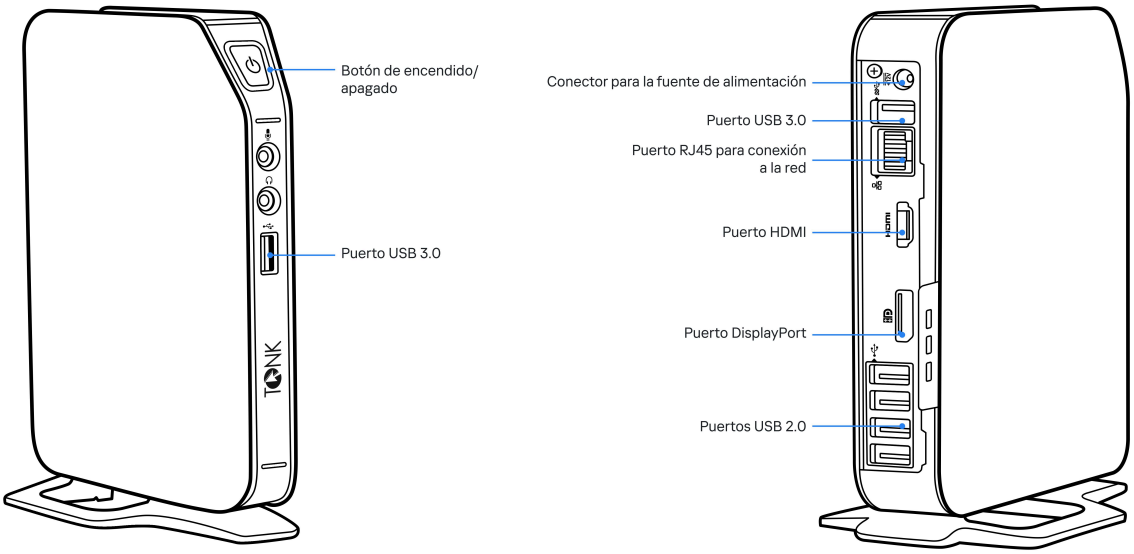
Para encender Kaspersky Thin Client:

Presione el botón de encendido y apagado, que se encuentra en la parte superior del panel frontal del cliente ligero.

Como resultado, Kaspersky Thin Client se pondrá en funcionamiento en el cliente ligero.

Durante el encendido y carga de Kaspersky Thin Client, el monitor conectado al cliente ligero mostrará secuencialmente la imagen de presentación del fabricante del cliente ligero, la pantalla de bienvenida del cargador de arranque, los registros de arranque y la imagen de presentación dinámica de Kaspersky Thin Client. La carga del sistema concluye cuando aparece la ventana principal de Kaspersky Thin Client en la pantalla.

Cuando Kaspersky Thin Client se inicia por primera vez, se muestra una ventana para aceptar el contrato de licencia de usuario final. Para continuar trabajando con Kaspersky Thin Client, primero es necesario leer detenidamente y aceptar el contrato de licencia de usuario final.



Paneles frontal y trasero del cliente ligero TONK TN1200

Cuando termine de trabajar con Kaspersky Thin Client, apague el sistema.

Para apagar Kaspersky Thin Client,

1. En la ventana principal de Kaspersky Thin Client, haga clic en el botón de apagado () ubicado en el panel de control.

2. En el menú que se abre, haga clic en **Apagar**.

Kaspersky Thin Client se apagará.

Reiniciar Kaspersky Thin Client

Puede reiniciar Kaspersky Thin Client si resulta necesario. Podría tener que reiniciar Kaspersky Thin Client si, por ejemplo, desea aplicar un nuevo idioma a la interfaz de Kaspersky Thin Client.

Para reiniciar Kaspersky Thin Client:

1. En la ventana principal de Kaspersky Thin Client, haga clic en el botón de apagado () ubicado en el panel de control.

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

Cuando un cliente ligero no está conectado a Kaspersky Security Center y el administrador no ha asignado certificados para el mismo en Web Console, quien utiliza ese cliente ligero puede aceptar o rechazar certificados en Kaspersky Thin Client a voluntad al conectarse a un entorno remoto o a un servidor de registros. 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.

Se recomienda 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 ayudarán a evitar que Kaspersky Thin Client se conecte a nodos que no sean de confianza.

Se recomienda 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 el administrador para configurar Kaspersky Thin Client y Kaspersky Security Center, así como para establecer una conexión entre estas dos soluciones.

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.

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 más información sobre la instalación de Kaspersky Security Center, consulte la sección *Instalación de Kaspersky Security Center* en la guía de 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 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 más información sobre cómo habilitar este puerto TCP en el Servidor de administración de Kaspersky Security Center, consulte la sección *Modificar la configuración de administración de dispositivos móviles* en la guía de ayuda en línea de Kaspersky Security Center.

5. **Encender Kaspersky Thin Client**

   Encienda Kaspersky Thin Client y espere a que se cargue el 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. **Agregar Kaspersky Thin Client a la lista de dispositivos administrados**

   Conéctese a Kaspersky Security Center Web Console y agregue Kaspersky Thin Client a la lista de dispositivos administrados con Kaspersky Security Center. Las directivas de Kaspersky Security Center Web Console se aplican solo a los dispositivos administrados.

9. **Crear una directiva activa de Kaspersky Security Center para Kaspersky Thin Client**

   Si necesita administrar un grupo de dispositivos, cree una directiva activa para Kaspersky Thin Client.

10. **Asignar los certificados de un grupo de dispositivos**

    Asigne los certificados necesarios para conectar un grupo de dispositivos 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 para 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 los clientes ligeros al grupo de dispositivos administrados**

   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 dispositivos administrados.

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 dispositivos pertinente.

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. El periodo de sincronización se define 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 más información sobre la instalación de Kaspersky Security Center, consulte la sección *Instalación de Kaspersky Security Center* en la guía de 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 más información sobre cómo habilitar este puerto TCP en el Servidor de administración de Kaspersky Security Center, consulte la sección *Modificar la configuración de administración de dispositivos móviles* en la guía de 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, guárdelo 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

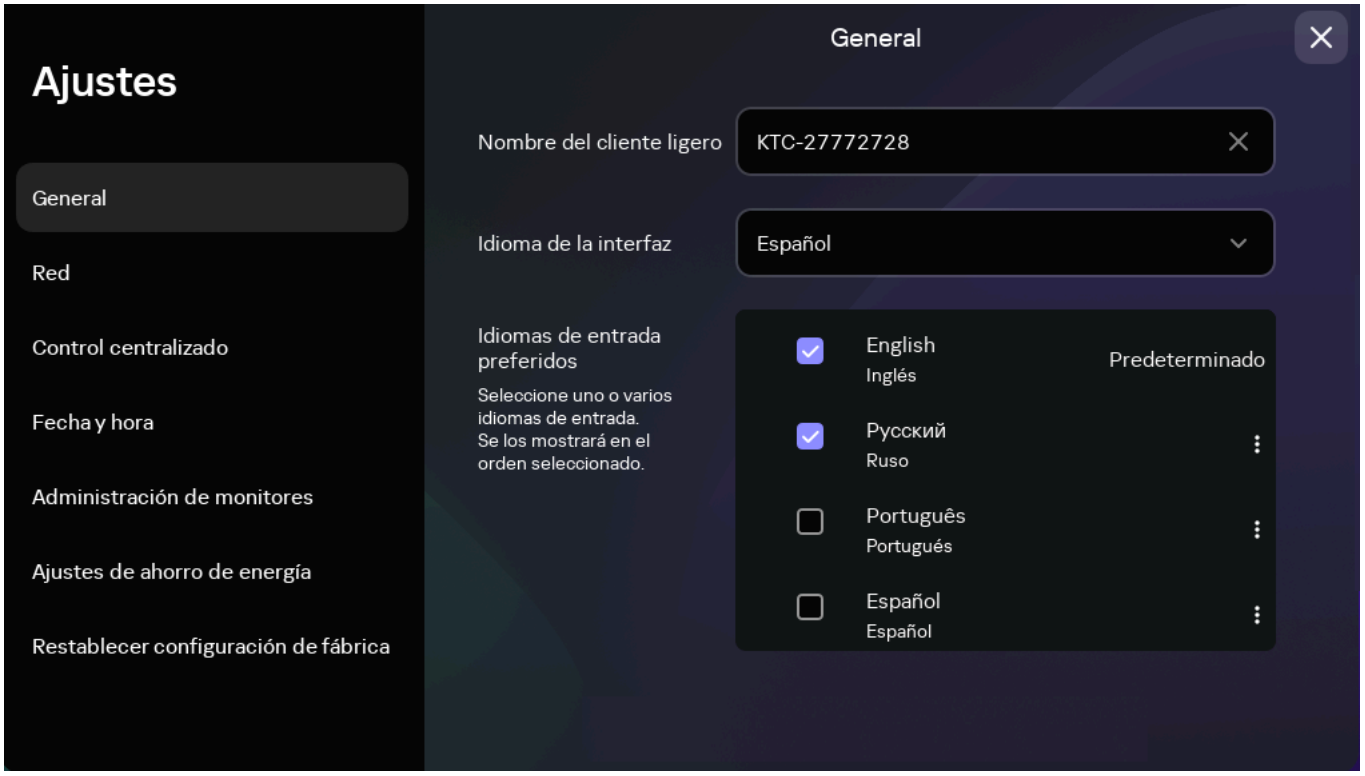
A través de la interfaz de Kaspersky Thin Client, puede configurar los ajustes generales del cliente ligero. Por ejemplo, puede definir el nombre que se muestra para el cliente ligero en la barra de tareas de Kaspersky Thin Client y en Kaspersky Security Center Web Console. También puede seleccionar 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 usuario de Kaspersky Thin Client está disponible en ruso, inglés, español y portugués de Brasil.
5. En la lista desplegable **Idiomas de entrada preferidos**, seleccione uno o más idiomas. Kaspersky Thin Client admite los idiomas de entrada ruso, inglés, español y portugués de Brasil. 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.

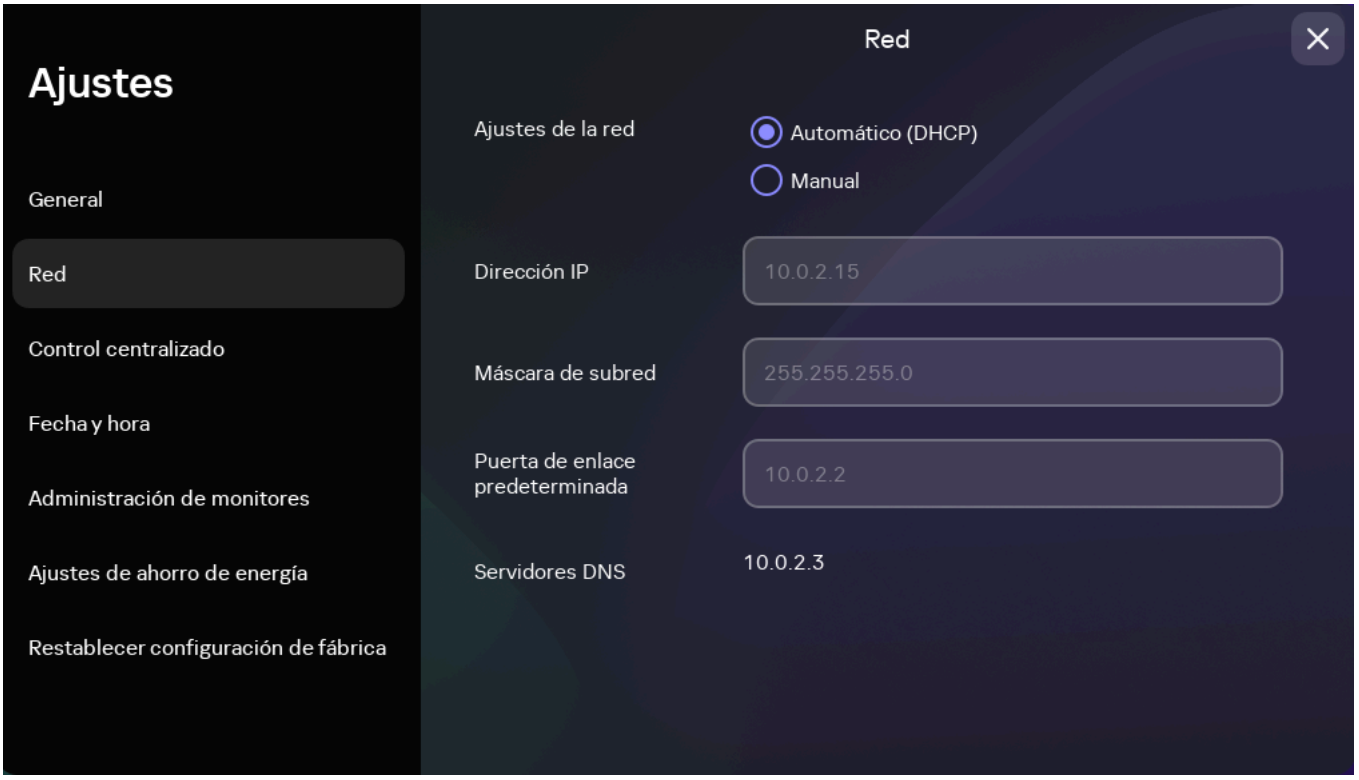
Configurar los ajustes de la red

En la sección **Ajustes** → **Red**, 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 **Ajustes 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 **Ajustes 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. Este campo es opcional.

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

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

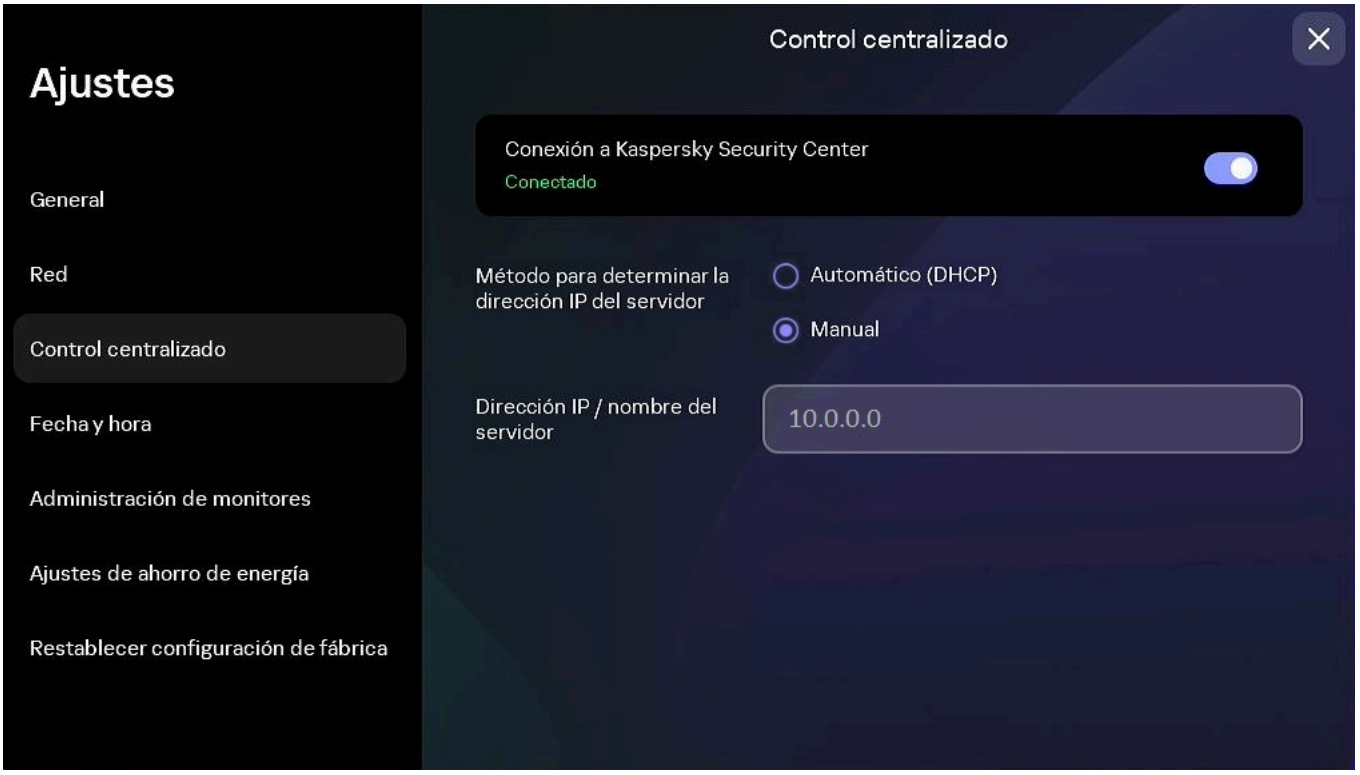
Para controlar un cliente ligero a través de Web Console, debe configurar los ajustes que permiten conectar Kaspersky Thin Client al Servidor de administración de Kaspersky Security Center.

Kaspersky Thin Client debe conectarse al Servidor de Kaspersky Security Center a través de un segmento de red seguro. Recomendamos configurar la conexión con la ayuda de un especialista cualificado de su empresa, que pueda 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 los ajustes para conectarse a un entorno remoto a través de RDP

Kaspersky Thin Client le permite configurar los ajustes para conectarse a una aplicación virtual o a un escritorio remoto a través de RDP.

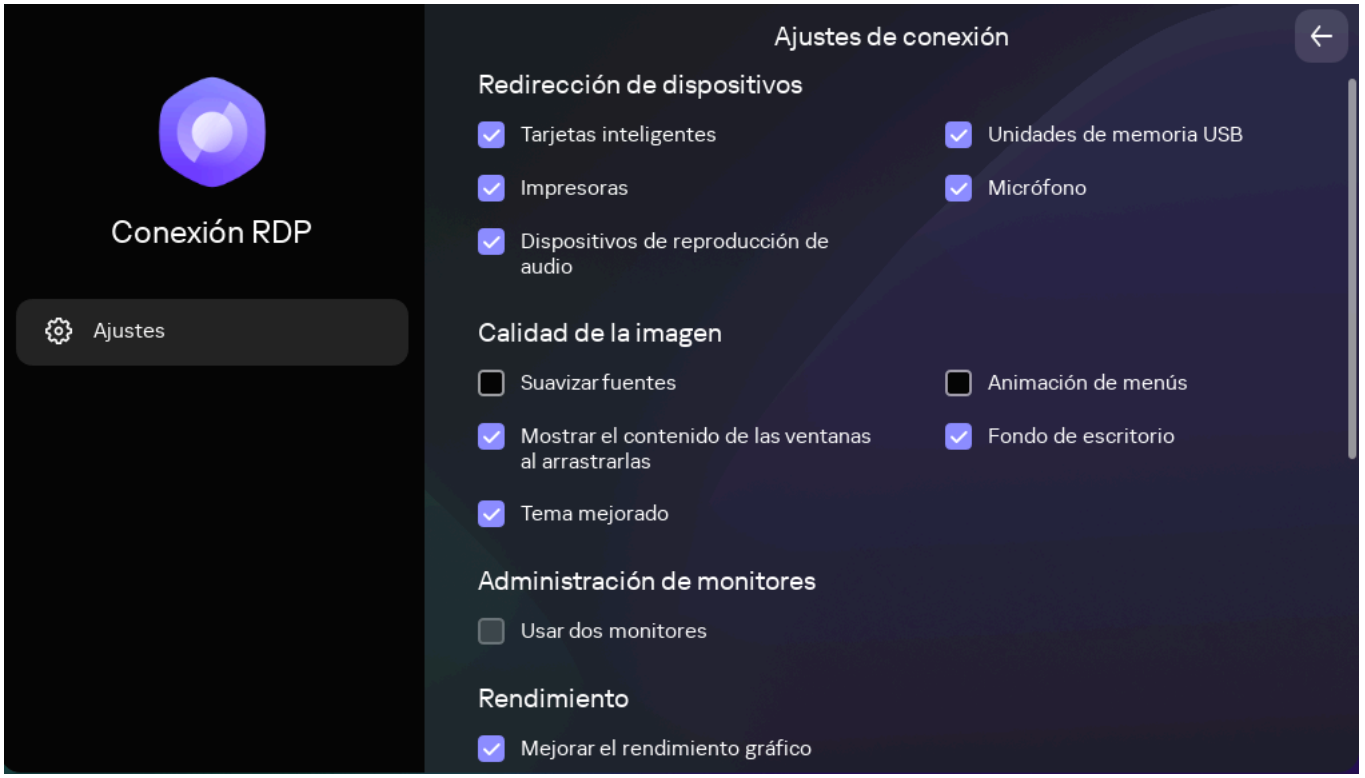
Para ver información sobre los dispositivos redireccionados a un entorno remoto, consulte este otro artículo.

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 sistemas operativos Microsoft Windows Server 2016 y Microsoft Windows Server 2019, también se debe habilitar la conexión remota a través de los Servicios de escritorio remoto y permitir que se establezcan reglas de control remoto para las sesiones de conexión de los Servicios de escritorio remoto.

Para configurar los ajustes para conectarse a un escritorio remoto o una aplicación virtual a través de RDP:

1. En la ventana principal 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 a un escritorio remoto (vea la siguiente imagen).



Ventana para configurar los ajustes aplicados al conectarse a un escritorio remoto a través de RDP

3. En el bloque **Redirección de dispositivos**, marque las casillas adyacentes a los dispositivos que corresponda:

   - Marque **Tarjetas inteligentes** si desea habilitar la redirección de tarjetas inteligentes y tókenes.
   - Marque **Unidades de memoria USB** si desea habilitar la redirección de unidades de memoria USB.
   - Marque **Impresoras** si desea habilitar la redirección de impresoras.

     La computadora remota deberá tener instalado el controlador de la impresora conectada al cliente ligero.
   - **Micrófono** si desea habilitar la redirección de dispositivos de grabación de audio.

     El volumen de audio y otras configuraciones se administran desde el equipo remoto.
   - **Dispositivos de reproducción de audio** si desea habilitar la redirección de auriculares o altavoces.

     Kaspersky Thin Client puede reproducir audio mono y estéreo. El volumen del audio y otros ajustes se controlan desde el entorno remoto.

4. En el bloque **Calidad de la imagen**, marque las casillas ubicadas junto a los ajustes de gráficos del escritorio remoto que desee 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**. Si es necesario, puede configurar la disposición de los monitores.

6. Si desea que los elementos gráficos se muestren mejor y con mayor fluidez cuando se conecte a un entorno remoto, marque la casilla **Mejorar el rendimiento gráfico** en el bloque **Rendimiento**.

   Si precisa conectarse a un escritorio remoto que ejecute Microsoft Windows 7, desmarque la casilla **Mejorar el rendimiento gráfico**. La función no es compatible con las conexiones a escritorios remotos que ejecuten Microsoft Windows 7.

7. 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).

   Ingrese un identificador de colección del Agente de conexión a Escritorio remoto para conectarse a una aplicación virtual.

8. 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 ubicada en la esquina superior derecha de la ventana para regresar a la sesión de conexión.

Configurar los ajustes para conectarse a un entorno remoto mediante la infraestructura de Basis.WorkPlace

Kaspersky Thin Client le permite configurar los ajustes para conectarse a un entorno remoto mediante la infraestructura de Basis.WorkPlace.

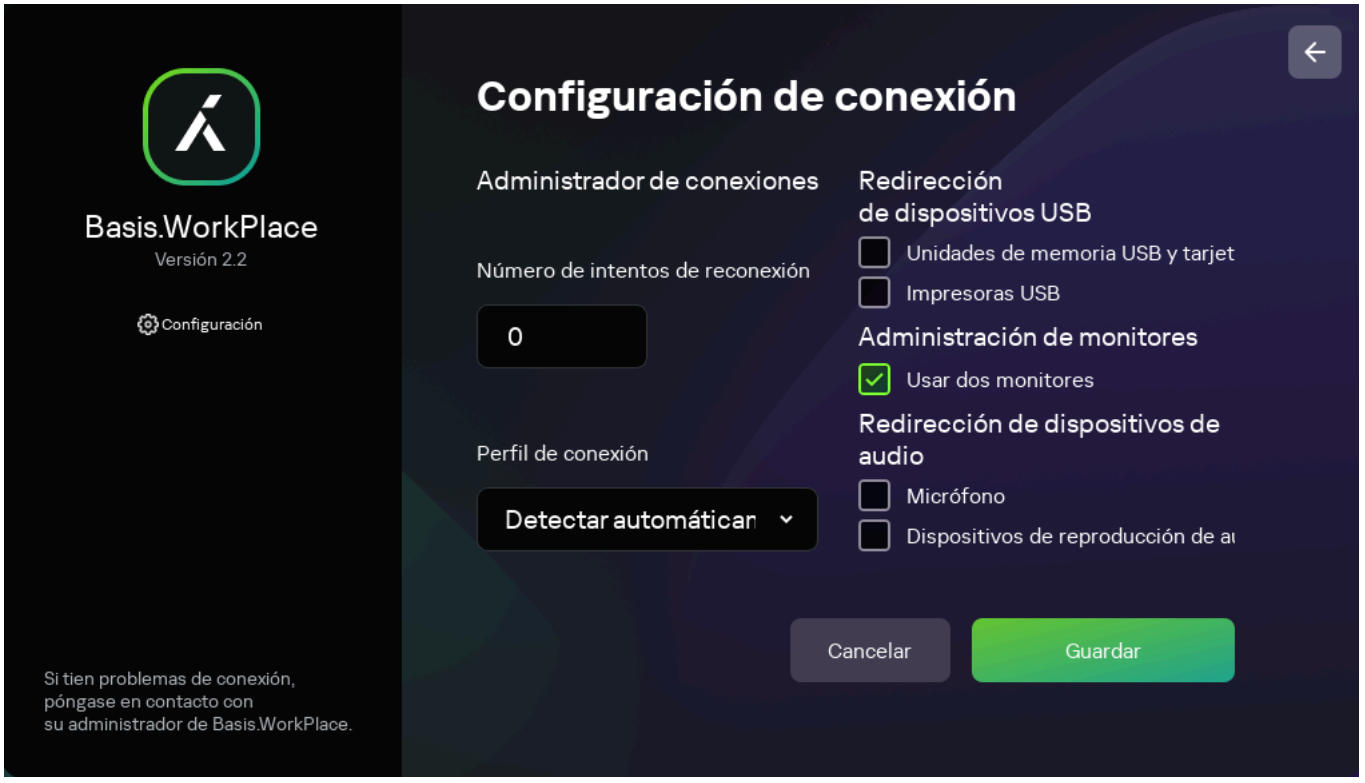
Para ver información sobre los dispositivos redireccionados a un entorno remoto, consulte este otro artículo.

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

1. En la ventana principal 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 **Configuración**.

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



Ventana para configurar los ajustes para conectarse a un escritorio remoto administrado por Basis.WorkPlace

3. Si desea habilitar o deshabilitar la redirección de dispositivos al entorno remoto, marque o desmarque las casillas correspondientes en el bloque **Redirección de dispositivos USB**.

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

4. 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.

5. 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**

6. 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**. Si es necesario, puede configurar la disposición de los monitores.

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

8. Haga clic en la flecha hacia atrás en la esquina superior derecha de la ventana para regresar a la ventana de conexión al escritorio remoto.

Configurar los ajustes de ahorro de energía

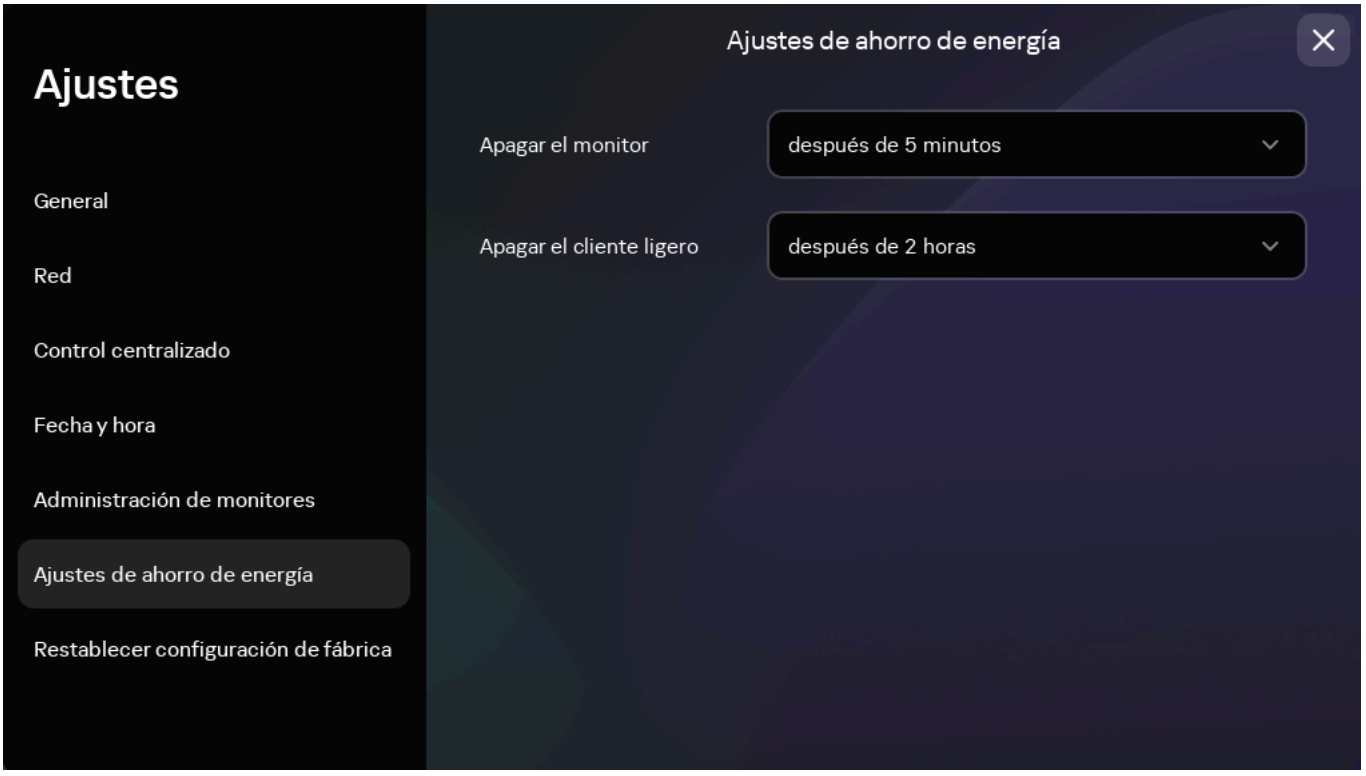
Cuando un cliente ligero forma parte de un grupo de administración, los valores de los ajustes que se detallan en este artículo se pueden imponer a través de Web Console. De ser este el caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

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 y, 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 la disposición de los monitores

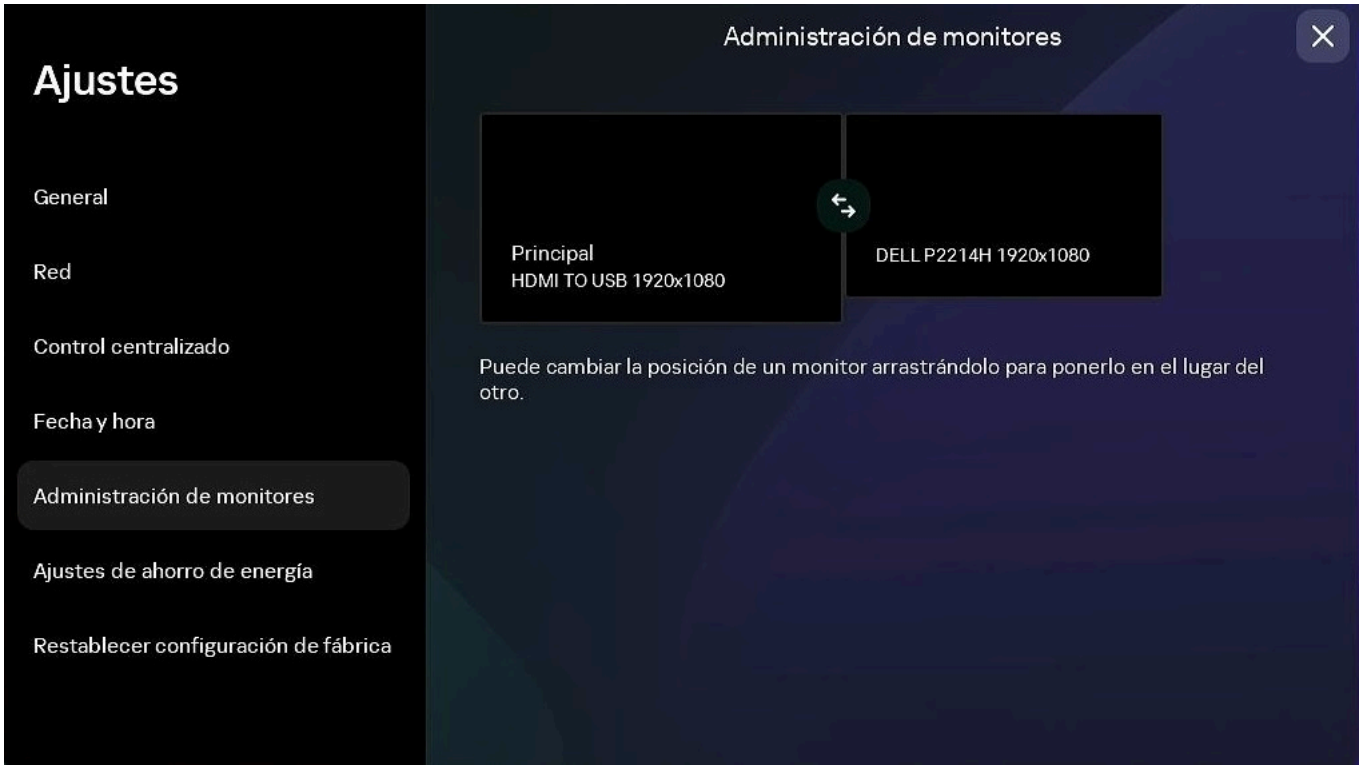
Si su estación de trabajo tiene dos monitores, puede indicar cuál deberá usarse como monitor principal y cuál como monitor secundario para mostrar la pantalla del escritorio remoto. Cuando se conecte al escritorio remoto, el panel de conexión se mostrará en la parte superior del monitor principal.

Para usar dos monitores, primero debe habilitar la compatibilidad con dos monitores en los ajustes de conexión a escritorios remotos, ya sea para conexiones RDP o para escritorios administrados por Basis.WorkPlace.

Para cambiar la disposición de los monitores en los que se muestra el escritorio remoto:

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).

   La ventana que se abre muestra un esquema con la posición de los monitores. El monitor principal siempre se encuentra a la izquierda y está identificado como tal.



Ajustes. Sección **Administración de monitores**

3. Para cambiar la posición de los monitores, haga clic en el botón ubicado entre los monitores del esquema.

   Se cambiará la disposición de los monitores en los que se muestra el escritorio 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:

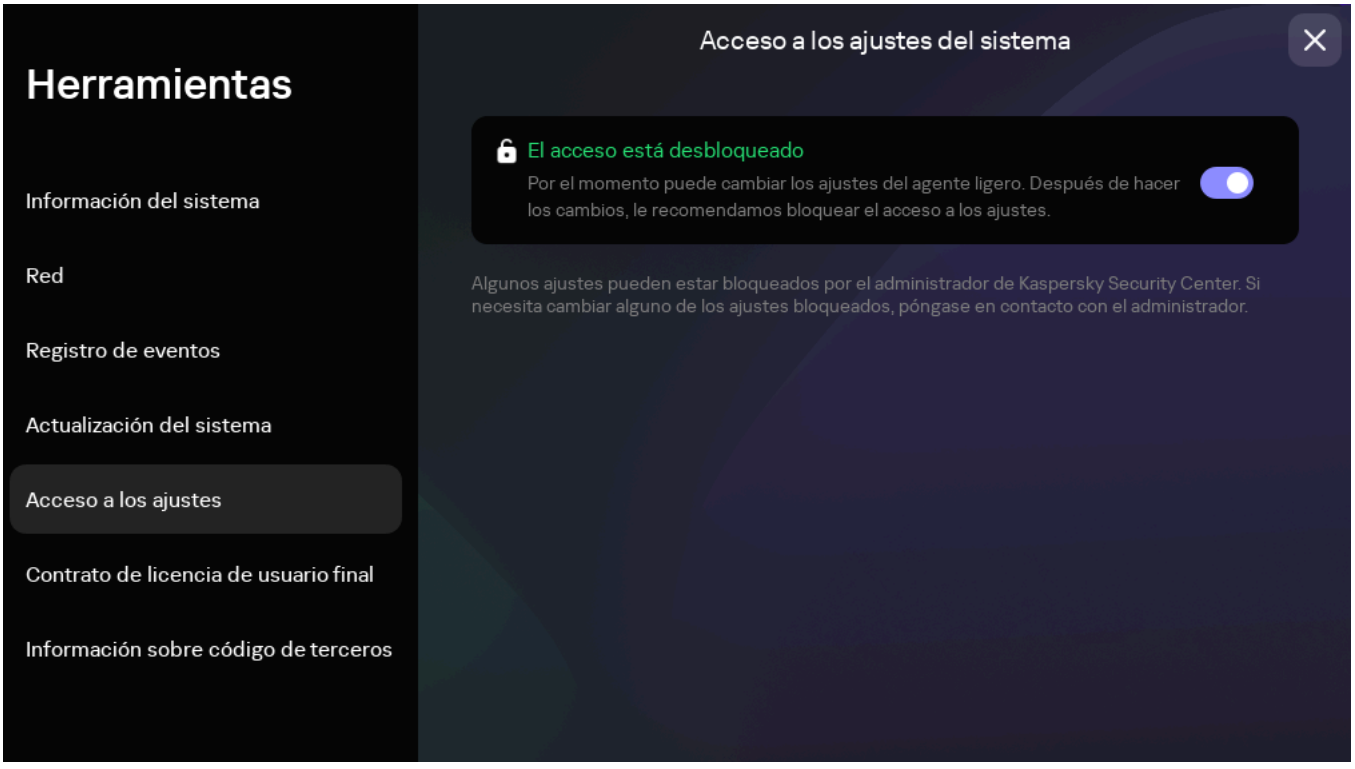
   - Si desea ocultar los ajustes, ponga el interruptor en la posición **El acceso está bloqueado**.

     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 **El acceso está desbloqueado**.

     Se mostrarán los ajustes. Podrá asignarles nuevos valores.



Herramientas. Sección **Acceso a los ajustes**

Configurar la fecha y la hora

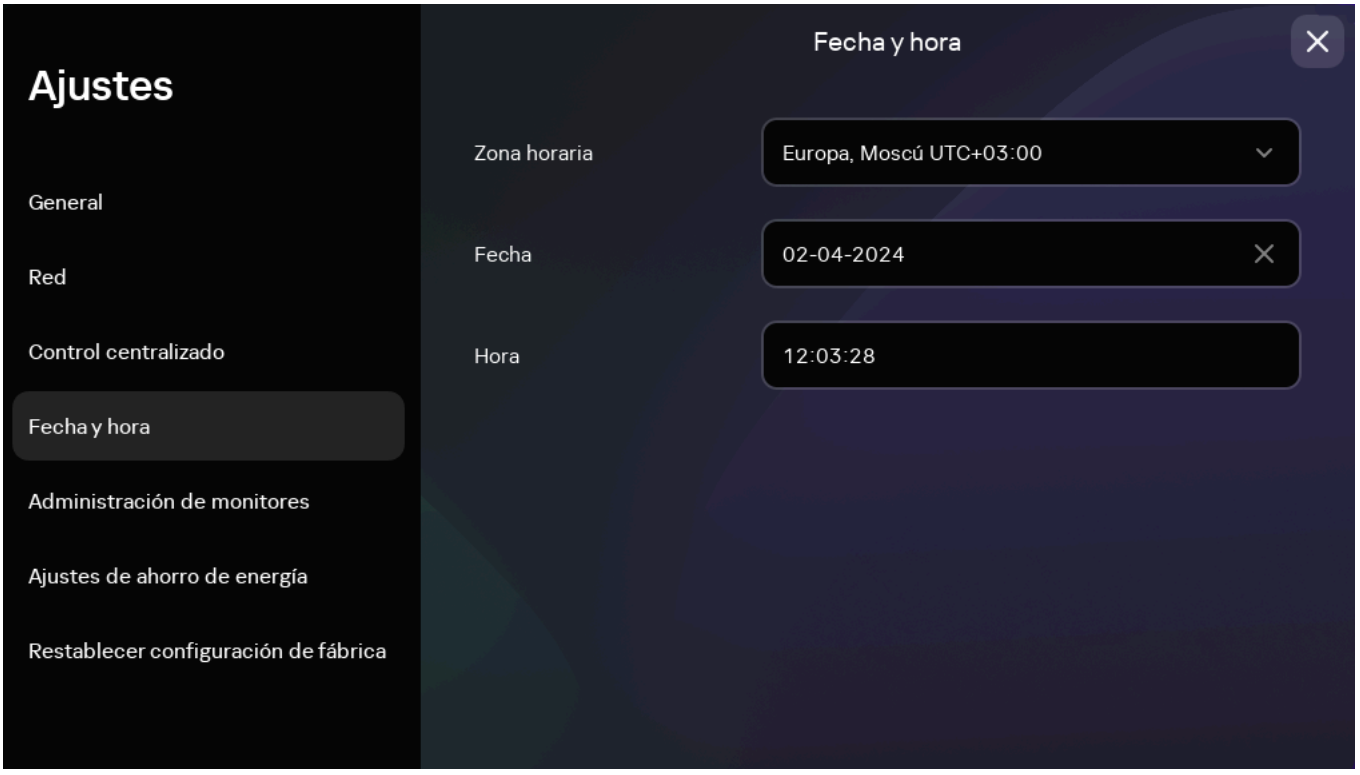
Los clientes ligeros conectados a Kaspersky Security Center obtienen la fecha y la hora del Servidor de administración de Kaspersky Security Center. Puede cambiar manualmente la fecha y la hora en Kaspersky Thin Client únicamente si el sistema no se controla a través de Kaspersky Security Center.

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 y, 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.

Restablecer la configuración de Kaspersky Thin Client

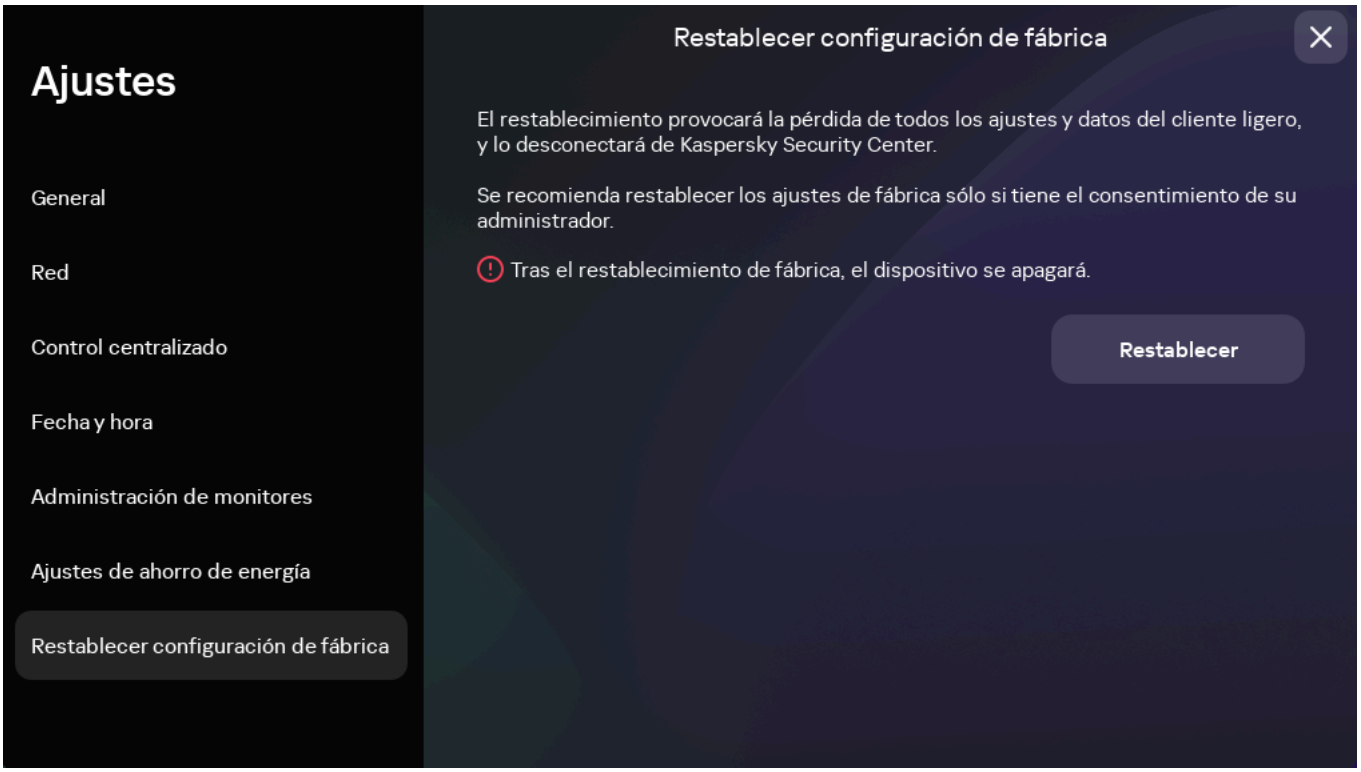
Cuando se lleva a cabo un restablecimiento, se eliminan todos los ajustes definidos y todos los datos de Kaspersky Thin Client (excepto el registro de auditoría y la fecha del sistema). También se desconecta el dispositivo de Kaspersky Security Center. Recomendamos llevar a cabo un restablecimiento solo 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 pueden imponerse a través de Web Console. De ser este el caso, no podrá configurar estos ajustes en la interfaz de Kaspersky Thin Client.

Los ajustes que se detallan en este artículo podrían no ser visibles en el cliente ligero.

Para restablecer la configuración de fábrica de un cliente ligero que no 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** (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.

Administrar Kaspersky Thin Client en la interfaz del cliente ligero

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

El principal escenario de funcionamiento de Kaspersky Thin Client consta de los siguientes pasos:

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. **Iniciar la sesión de conexión**

   Conéctese a un entorno remoto y comience a trabajar.

4. **Bloquear el escritorio y retomar lo que se estaba haciendo**

   Si necesita alejarse un momento de la estación de trabajo, bloquee el escritorio remoto. Cuando regrese a la estación de trabajo, reanude sus tareas. Para obtener información detallada sobre cómo bloquear el escritorio remoto y retomar luego el trabajo, consulte el manual del sistema operativo remoto al que se conecte.

5. **Cerrar la sesión de conexión**

   Cierre la conexión al entorno remoto antes de apagar el cliente ligero.

6. **Apagar Kaspersky Thin Client**

   Apague el cliente ligero cuando termine la jornada.

Conectarse a un entorno remoto

Puede usar Kaspersky Thin Client para lo siguiente:

- Conectarse a un escritorio remoto a través de RDP

  Para conectarse a un escritorio remoto a través de RDP:

  1. Encienda Kaspersky Thin Client.
  2. En la ventana principal 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.

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

     Si es la primera vez que se conecta a un escritorio remoto y Kaspersky Thin Client no pertenece a ningún grupo de administración, se abrirá una ventana llamada **Agregar certificado**. Revise en esta ventana los parámetros del certificado agregado y haga clic en el botón **Agregar certificado**.

     La conexión se establecerá automáticamente si Kaspersky Thin Client forma parte de un grupo de administración gestionado mediante Kaspersky Security Center Web Console y el administrador de Kaspersky Security Center agregó de antemano un certificado que permita autenticar el servidor para ese grupo de administración.

     El certificado de autenticación del servidor se agregará al almacén de certificados del sistema de Kaspersky Thin Client y se usará en las conexiones subsiguientes.
  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 la ventana del escritorio remoto y comienza la sesión de conexión.

- Conectarse a una aplicación virtual a través de RDP

Para conectarse a una aplicación virtual a través de RDP:

1. Encienda Kaspersky Thin Client.
2. En la ventana principal 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.

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

   Si es la primera vez que se conecta a la aplicación virtual seleccionada y Kaspersky Thin Client no pertenece a ningún grupo de administración, se abrirá una ventana llamada **Agregar certificado**. Revise en esta ventana los parámetros del certificado agregado 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.

   Si el administrador de Kaspersky Security Center ya sumó Kaspersky Thin Client a un grupo de administración y agregó un certificado de autenticación de servidor para ese grupo, la conexión se establecerá automáticamente.

   Se abre la ventana de la aplicación virtual en ejecución y comienza la sesión de conexión.

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 escritorio remoto administrado por Basis.WorkPlace

Para conectarse a un escritorio remoto administrado por Basis.WorkPlace:

1. Encienda Kaspersky Thin Client.
2. En la ventana principal 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**, ingrese la dirección IP o el nombre de servidor del administrador de conexiones de Basis.WorkPlace.

      Kaspersky Thin Client guarda la dirección del último administrador de conexiones de Basis.WorkPlace con el que se establece correctamente una conexión, por lo 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 remoto. 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. Haga clic en el botón **Conectarse**.

   Si es la primera vez que se conecta a un escritorio remoto administrado por Basis.WorkPlace y Kaspersky Thin Client no pertenece a ningún grupo de administración, se abrirá una ventana llamada **Agregar certificado**. Revise en esta ventana los parámetros del certificado agregado y haga clic en el botón **Agregar certificado**.

   La conexión con el escritorio remoto administrado por Basis.WorkPlace se establecerá automáticamente si Kaspersky Thin Client ya forma parte de un grupo de administración gestionado mediante Kaspersky Security Center Web Console y el administrador de Kaspersky Security Center agregó de antemano un certificado para autenticar al agente de Basis.WorkPlace para ese grupo de administración.

   El certificado para autenticar al agente de Basis.WorkPlace se agregará al almacén de certificados del sistema de Kaspersky Thin Client y se usará en las subsiguientes conexiones.

   Se abre una ventana para seleccionar un escritorio remoto. La ventana muestra todos los escritorios a los que puede conectarse.

5. Si desea actualizar la lista de escritorios, haga clic en el botón **Recargar**.
6. Haga clic en el botón con el nombre del escritorio al que desee conectarse.

Después de unos segundos, verá en pantalla el escritorio remoto al que se haya conectado.

En la ventana para conectarse a los escritorios administrados por Basis.WorkPlace, también puede hacer clic en **Configuración** para configurar los ajustes de conexión.

El administrador de Basis.WorkPlace puede restringir el acceso a los escritorios administrados por Basis.WorkPlace. Entre otras acciones, el administrador puede bloquear una cuenta de usuario o determinar que una cuenta no pueda acceder a escritorios remotos administrados por Basis.WorkPlace a los que antes tuviera acceso. Si tiene problemas para conectarse a un escritorio remoto, recomendamos que se comunique con el administrador de Basis.WorkPlace.

- Conectarse 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 y VMware Horizon. Web Access admite HTML5 y proporciona una conexión HTTPS segura al conectarse.

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

1. Encienda Kaspersky Thin Client.
2. En la ventana principal de Kaspersky Thin Client, haga clic en **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. Haga clic en el botón **Conectarse**.

   Si es la primera vez que se conecta al entorno virtual y Kaspersky Thin Client no pertenece a ningún grupo de administración, se abrirá una ventana llamada **Agregar certificado**. Revise en esta ventana los parámetros del certificado agregado y haga clic en el botón **Agregar certificado**.

   La conexión con el entorno remoto se establecerá automáticamente si Kaspersky Thin Client ya forma parte de un grupo de administración gestionado mediante Kaspersky Security Center Web Console y el administrador de Kaspersky Security Center agregó de antemano un certificado para autenticar la dirección web del servidor para ese grupo de administración.

   El certificado para autenticar la dirección web del servidor se agregará al almacén de certificados del sistema de Kaspersky Thin Client y se usará para futuras conexiones.

   Si solo hay un escritorio remoto al que puede conectarse, su monitor mostrará el escritorio remoto al que está conectado. Si hay varios escritorios remotos a los que puede conectarse, se abrirá una ventana de selección que muestra todos los escritorios remotos disponibles para la conexión.

   Los datos que se necesiten para usar el entorno remoto, incluidas las cookies, se almacenarán en el cliente ligero hasta que se cierre la conexión remota. Los datos se eliminarán una vez que finalice la conexión.

5. Si desea actualizar la lista de escritorios remotos, haga clic en el botón **Recargar**.
6. Haga clic en el botón con el nombre del escritorio remoto al que desee conectarse.

Después de unos segundos, verá en pantalla el escritorio remoto al que se haya conectado.

No se permite tener más de una sesión de conexión activa a la vez.

Kaspersky Thin Client utiliza el cifrado TLS para proteger todas las sesiones de conexión y evitar que los datos sean interceptados o reemplazados.

Utilizar el panel de conexión

El panel de conexión aparece en la parte superior de la pantalla cuando se establece conexión con un entorno remoto. Se lo utiliza para administrar la sesión de conexión activa.

Para administrar una sesión de conexión remota mediante el panel de conexión, haga lo siguiente:

1. Para cerrar la sesión de conexión remota, haga clic en **Desconectarse del servidor**.
2. Para cambiar el idioma en el que se muestra la interfaz del cliente ligero, haga clic en el nombre abreviado del idioma que esté utilizando y, en la lista desplegable, seleccione el idioma que desee utilizar.
3. Para ver información sobre el servicio de Soporte técnico, haga clic en .

El panel de conexión se contrae automáticamente cuando pierde el foco del teclado o el mouse.

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

Haga clic en el ícono de la aplicación en el panel de conexión y, en la lista desplegable, seleccione la ventana pertinente.

Para contraer o restaurar el panel de conexión, haga lo siguiente:

1. Para restaurar el panel de conexión, haga clic en el panel contraído o presione **`Ctrl + Alt + Inicio`**.
2. Para contraer el panel de conexión si tiene el foco del teclado, presione **`Esc`**.
3. Para contraer el panel de conexión sin quitarle el foco a la ventana de la sesión remota, presione **`Ctrl + Alt + Inicio`**.

Cuando está contraído, el panel de conexión puede desplazarse horizontalmente hacia la derecha o hacia la izquierda.

Para cambiar la posición del panel de conexión:

Haga clic en el área sin botones del panel de conexión y, utilizando el mouse, arrastre el panel.

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

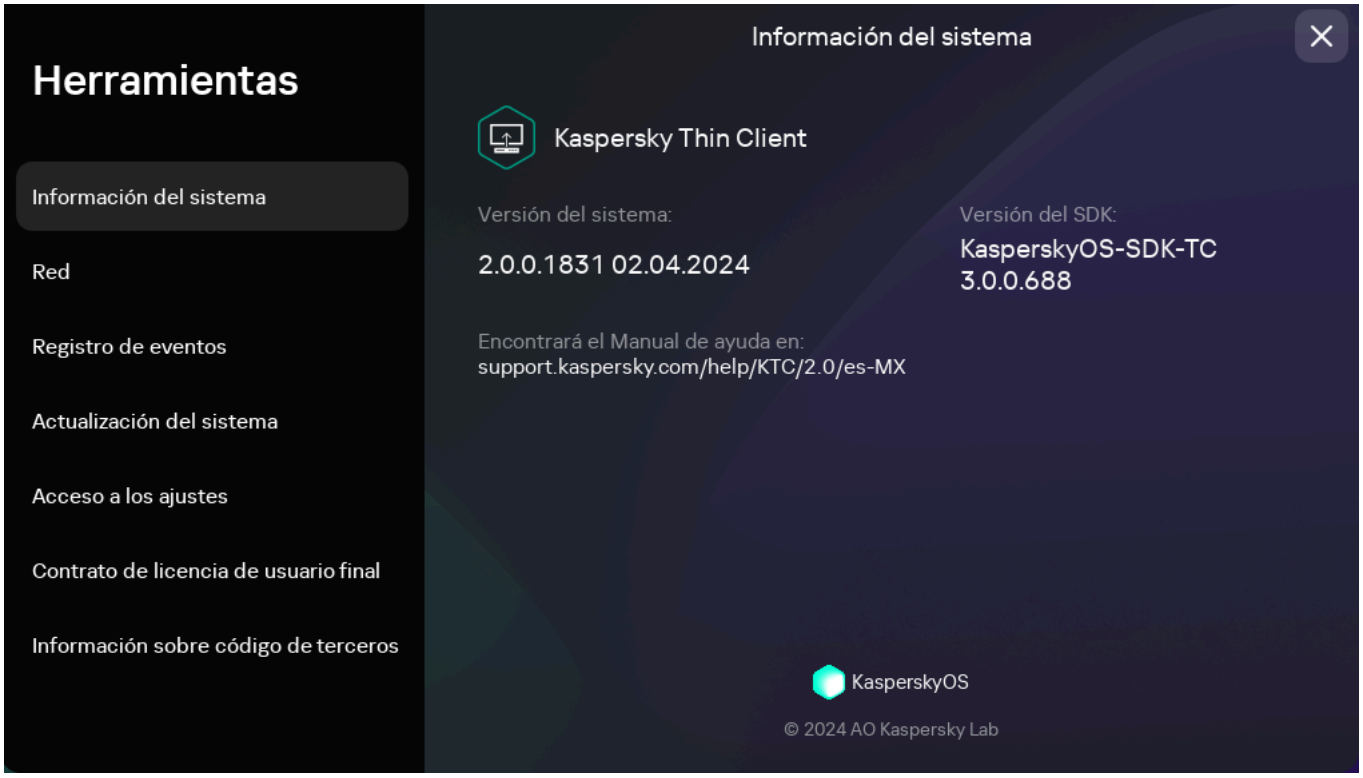
Para controlar el panel de conexión y la sesión remota, también puede utilizar teclas de acceso rápido.

Ver información sobre Kaspersky Thin Client

Puede ver información sobre Kaspersky Thin Client en **Herramientas** → **Información del sistema**.

La sección **Información del sistema** muestra los siguientes datos:

- Número de versión de Kaspersky Thin Client
- Número de versión de KasperskyOS
- Vínculo a la ayuda en línea de Kaspersky Thin Client



Herramientas. Sección **Información del sistema**

Ver información sobre el estado de la red

A través de **Herramientas** → **Red**, puede ver el estado de la red y los valores de la conexión de red de Kaspersky Thin Client. La información sobre los valores de la conexión de red de Kaspersky Thin Client se actualiza automáticamente al menos una vez por segundo.

La sección **Red** brinda la siguiente información sobre los valores de la conexión de red de Kaspersky Thin Client (vea la imagen más abajo):

- **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.
- Una solicitud 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.

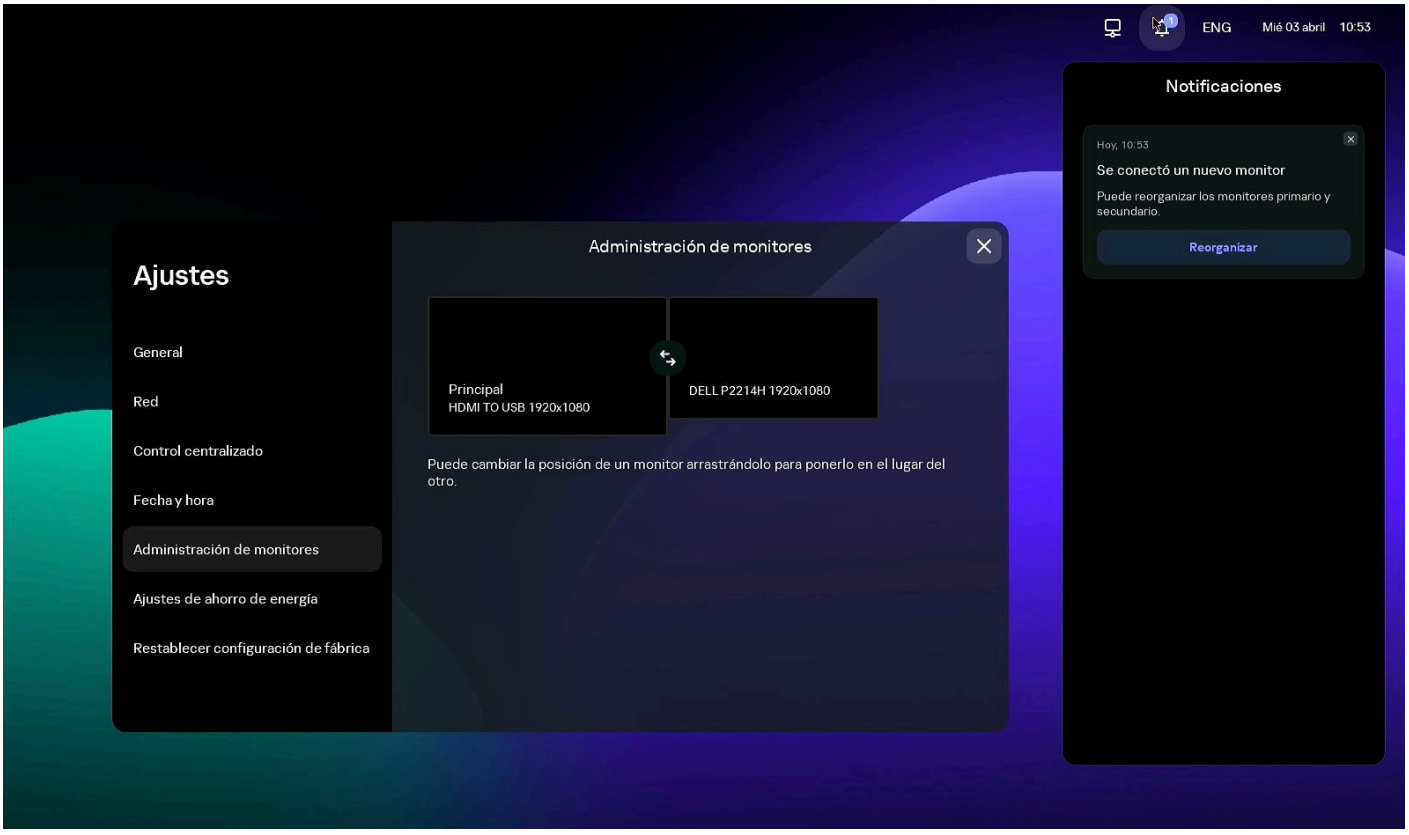
Si el cursor o el foco del teclado están fuera del área de notificación, las solicitudes no resueltas y no leídas se ocultan y el contador en el panel de control muestra su número.

Cuando hay una sesión de conexión activa, las notificaciones sobre actualizaciones no se ocultan automáticamente. Puede cerrar estas notificaciones manualmente o puede seleccionar la acción pertinente para cerrarlas.

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 una lista de notificaciones si hay alguna nueva notificación disponible (vea la siguiente imagen).



Panel de notificaciones de Kaspersky Thin Client

Administrar certificados en la interfaz del cliente ligero

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 proporcióneselo 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 de 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. Se recomienda 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. Estas medidas ayudarán 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.

Cerrar la sesión de conexión

Para cerrar una sesión de conexión remota:

Restaure el panel de conexión y haga clic en el elemento **Desconectarse del servidor** del panel.

La sesión se cierra y aparece una ventana de conexión.

Administrar Kaspersky Thin Client mediante combinaciones de teclas

Existen teclas de acceso rápido y combinaciones de teclas específicas que puede utilizar en Kaspersky Thin Client y durante las sesiones de conexión. La siguiente tabla enumera todas las teclas de acceso rápido y combinaciones de teclas disponibles.

Teclas de acceso rápido y combinaciones de teclas para Kaspersky Thin Client

Teclas y combinaciones de teclas	Acciones
Windows	Abrir o cerrar el menú de apagado.
→ ←	Alternar entre las opciones de conexión disponibles (**RDP**, **Basis.WorkPlace** y **Web Access**) en la ventana principal de Kaspersky Thin Client.
↑ ↓	• Escoger entre los elementos de la lista desplegable. • Desplazar el contenido de la página hacia arriba o hacia abajo.
Tabulador	Desplazarse de *izquierda* a *derecha* o de *arriba abajo* 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 *derecha* a *izquierda* o de *abajo arriba* 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 de conexión. Este acceso directo solo puede utilizarse si el panel de conexión se ha expandido.
Win+|	Abrir la ventana **Ajustes** desde la ventana principal de Kaspersky Thin Client si el acceso a los ajustes no se ha bloqueado.
Win+U	Abrir la ventana **Herramientas** desde la ventana principal de Kaspersky Thin Client.
Win+Esc	Apagar Kaspersky Thin Client desde la ventana principal de Kaspersky Thin Client.

Teclas y combinaciones de teclas	Acciones
Win+**F12** o **Win**+**Fin**	Reiniciar Kaspersky Thin Client desde la ventana principal de Kaspersky Thin Client.
Win+**A** o **Win**+**N**	Abrir el panel de notificaciones desde la ventana principal 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.

Actualizar Kaspersky Thin Client en la interfaz del cliente ligero

Para actualizar Kaspersky Thin Client, el cliente ligero debe estar conectado a Kaspersky Security Center.

Una vez que las actualizaciones se han descargado en el dispositivo, aparece una notificación en la interfaz de Kaspersky Thin Client con la hora en la que se aplicará la actualización.

Puede instalar una actualización de una de las siguientes maneras:

- Directamente desde la notificación sobre la actualización disponible

  - Si desea instalar la actualización en el momento en que aparece la notificación, haga clic en el botón **Reiniciar ahora** en la ventana de notificación sobre la actualización disponible.

    Se instalarán las actualizaciones y se reiniciará Kaspersky Thin Client.

  - Si desea instalar las actualizaciones en otro momento, haga clic en **Más tarde** en la ventana de notificación sobre la actualización disponible. La notificación le indicará por cuánto tiempo se pospondrá la instalación. El administrador define a qué hora se realizará la instalación pospuesta.

    Se pospondrán el reinicio y la actualización del sistema.

    Si ignora o cierra la notificación de actualización de Kaspersky Thin Client varias veces, la actualización se instalará automáticamente.

- Al reiniciar o apagar el cliente ligero

  1. En el panel de control de Kaspersky Thin Client, haga clic en el botón de apagado ( ).
  2. Realice una de estas acciones, dependiendo de si precisa seguir trabajando con Kaspersky Thin Client tras la actualización:

     - Si precisa seguir trabajando, seleccione **Actualizar y reiniciar** en el menú que se abre.

       Se instalarán las actualizaciones y se reiniciará Kaspersky Thin Client.

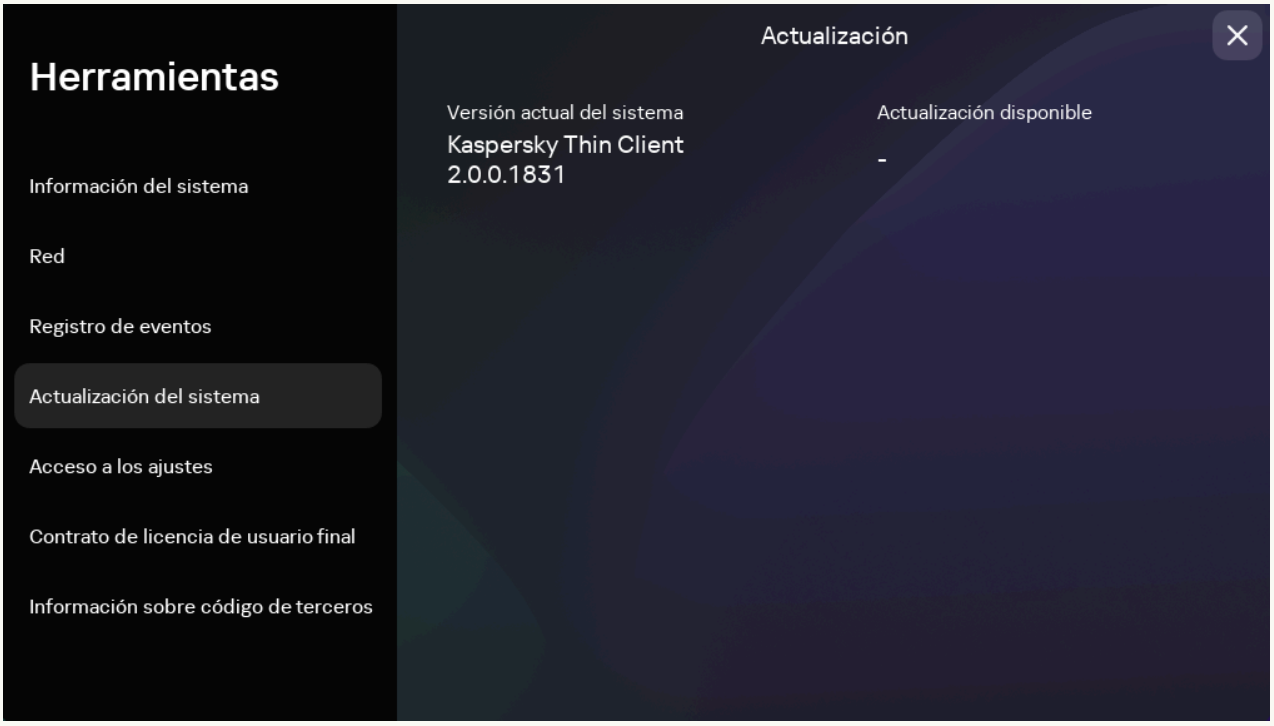
     - Si piensa dejar de trabajar, seleccione **Actualizar y apagar** en el menú que se abre.

       Se instalarán las actualizaciones y Kaspersky Thin Client se apagará.

- Desde la sección Actualización del sistema

  1. En el panel de control de Kaspersky Thin Client, haga clic en y, en el menú que se abre, seleccione **Herramientas**.
  2. Elija la sección **Actualización del sistema**.

Se abre una ventana con información sobre la versión del sistema instalada y las actualizaciones descargadas (vea la siguiente imagen).



Herramientas. Sección **Actualización del sistema**

3. Haga clic en **Instalar y reiniciar**. Si no hay ninguna actualización disponible, no verá este botón.

   Se instalarán las actualizaciones y se reiniciará Kaspersky Thin Client.

Si se descarga una actualización de Kaspersky Thin Client, pero usted no reinicia el sistema, la actualización se instalará automáticamente la siguiente vez que reinicie o apague el dispositivo.

La información detallada sobre la actualización centralizada de clientes ligeros mediante Web Console se proporciona en un artículo aparte.

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 ayuda en línea de Kaspersky Security Center Web Console.

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 los ajustes de Kaspersky Thin Client.
- Recibir y ver eventos de Kaspersky Thin Client.
- 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:

- Al configurar Kaspersky Thin Client, defina los ajustes que permitirán la conexión a Kaspersky Security Center.
- En Kaspersky Security Center Web Console, instale el complemento web de Kaspersky Security Management Suite.

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 detalles sobre la habilitación de puertos en un Servidor de administración de Kaspersky Security Center, consulte la sección *Modificar la configuración de administración de dispositivos móviles* de la guía de ayuda en línea de Kaspersky Security Center.

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 el menú de Web Console, 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 digital (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 el dispositivo del grupo 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 detalles sobre la configuración del acceso basado en roles, consulte la sección *Configurar los derechos de acceso a las funciones de la aplicación. Control de acceso basado en roles* en la guía de ayuda en línea de Kaspersky Security Center.

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

- *Oficial de seguridad*. Este rol tiene los permisos necesarios para ver todas las secciones de Kaspersky Security Management Suite y para administrar los certificados de Kaspersky Thin Client. Puede asignar este rol al empleado responsable de la seguridad de la información en la empresa.

- *Administrador*. Este rol tiene los permisos necesarios para ver todas las secciones de Kaspersky Security Management Suite y para administrar los ajustes de conexión a escritorios remotos, los ajustes generales, los ajustes del sistema y los datos de Kaspersky Thin Client. Puede asignar este rol al empleado responsable de mantener y administrar los sistemas de la información en la empresa.

- *Administrador avanzado*. Este rol tiene los permisos necesarios para ver y administrar todas las secciones de Kaspersky Security Management Suite y para administrar los certificados, los ajustes de conexión a escritorios remotos, los ajustes generales, los ajustes del sistema y los datos de Kaspersky Thin Client. 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.

En la siguiente tabla, se describen las funciones a las que tiene acceso el usuario dependiendo del rol que se le asigna para administrar Kaspersky Thin Client. 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	✓	–	✓
Configurar los ajustes de conexión a escritorios remotos 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	–	✓	✓

Iniciar y cerrar sesión en Web Console

Para iniciar sesión en Web Console, solicite al administrador la dirección web del Servidor de administración de Kaspersky Security Center y el número de puerto que se haya indicado durante la instalación (el puerto 8080 es el predeterminado). Asimismo, habilite JavaScript en el navegador.

Para iniciar sesión en Web Console:

1. En el navegador, vaya a `https://<dirección del Servidor de administración>:<número de puerto>`. 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 guía de ayuda en línea de Kaspersky Security Center Web Console.

   Se abre la página de inicio de sesión.

2. Inicie sesión con el nombre de usuario y la contraseña de un administrador local.

   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. Si es su primer inicio de sesión en Web Console, se abrirá el Asistente de inicio rápido. Para obtener más información sobre el funcionamiento de Kaspersky Security Center Web Console, consulte la guía de ayuda en línea de Kaspersky Security Center Web Console.

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.

Agregar un cliente ligero al grupo de dispositivos administrados

A través de Web Console, puede controlar de manera centralizada los clientes ligeros que se encuentren conectados a Kaspersky Security Center. Entre otras acciones, puede agregar los clientes ligeros a grupos de administración y aplicar las directivas que considere necesarias. Para controlar un cliente ligero en forma centralizada, primero debe agregarlo al grupo de dispositivos administrados.

Para agregar un cliente ligero al grupo de dispositivos administrados:

1. En la ventana principal de Web Console, seleccione **Descubrimiento y despliegue → Dispositivos no asignados**.

   Se mostrará una lista con todos los dispositivos no asignados que se hayan detectado.

2. Marque la casilla ubicada junto al nombre del dispositivo que desee agregar al grupo de dispositivos administrados.
3. Haga clic en el botón **Mover a un grupo**.

   Del lado derecho, se abrirá el panel **Mover a un grupo**. Marque la casilla ubicada junto al grupo de administración **Dispositivos administrados**.

4. Haga clic en el botón **Mover**.

El cliente ligero se agregará al grupo de dispositivos administrados.

Administrar directivas

Una *directiva* es un conjunto de ajustes operativos de Kaspersky Thin Client definidos para un grupo de administración. Puede configurar varias directivas con diferentes valores para un mismo dispositivo. La configuración de la aplicación puede variar de un grupo de administración a otro. Cada grupo de administración puede tener su propia directiva para la aplicación. Si desea información más detallada sobre el uso de las directivas de Kaspersky Security Center para administrar la aplicación, consulte la sección *Directivas y perfiles de directivas* en la guía de ayuda en línea de Kaspersky Security Center.

Los ajustes de una directiva se definen en Kaspersky Security Center Web Console, a través del complemento web, y se transmiten a Kaspersky Thin Client cuando la aplicación se sincroniza con Kaspersky Security Center. La frecuencia de sincronización puede modificarse en la configuración de la directiva.

Directivas activa e inactiva

Una directiva está pensada para un grupo de dispositivos administrados y puede estar activa o inactiva. Los ajustes de la directiva activa se guardan en los dispositivos cliente cuando se realiza la sincronización. No es posible aplicar varias directivas simultáneamente a un mismo dispositivo; en consecuencia, cada grupo puede tener solamente una directiva activa.

Puede crear todas las directivas inactivas que desee. Las directivas inactivas no modifican los ajustes de la aplicación en los dispositivos de la red. Están pensadas para utilizarse como preparativos para situaciones de emergencia, como un ataque de virus. Por ejemplo, ante un ataque con unidades de memoria USB, podría activar una directiva que impida el acceso a ese tipo de unidades. En tal caso, la directiva activa cambiará de estado a inactiva automáticamente.

Herencia de configuración

Las directivas, al igual que los grupos de administración, se organizan en una jerarquía. De manera predeterminada, una directiva secundaria hereda la configuración de su directiva principal. Una *directiva secundaria* es una directiva para niveles anidados de la jerarquía. En otras palabras, es una directiva para grupos de administración anidados y servidores de administración secundarios. De ser necesario, puede evitar que una directiva secundaria herede la configuración de su directiva principal.

En las directivas, cada ajuste tiene el atributo, que indica si el valor del ajuste se puede modificar en las directivas o en la configuración local de la aplicación. Dependiendo del estado de este atributo, verá uno de los siguientes valores junto a cada ajuste:

- Sin definir **Sin definir**. Cuando un ajuste tiene a su lado un candado abierto y el interruptor está desactivado, el valor de dicho ajuste no está definido en la directiva. El usuario puede modificar el valor del ajuste en la interfaz local de la aplicación de Kaspersky. Estos ajustes se denominan "desbloqueados".

- Imponer **Imponer**. Cuando un ajuste tiene a su lado un candado cerrado y el interruptor está activado, el valor definido para ese ajuste es el que se aplica en los dispositivos sujetos a la directiva. El usuario no puede cambiar el valor del ajuste en la interfaz local de la aplicación de Kaspersky. Estos ajustes se denominan "bloqueados".

El atributo se aplica a una directiva secundaria solo si se ha indicado que esa directiva debe heredar la configuración de su directiva principal.

Crear una directiva

Para administrar un grupo de dispositivos con Kaspersky Thin Client a través de Web Console, debe crear una directiva.

Para crear una directiva para un grupo de dispositivos:

1. En la ventana principal de Web Console, seleccione **Dispositivos → Directivas y perfiles**.
2. Haga clic en el botón **Agregar**.
3. En la ventana que se abre, en la lista de aplicaciones, seleccione Kaspersky Security Management Suite y haga clic en **Siguiente**.
4. 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. De forma predeterminada, el campo muestra el nombre del complemento web de administración de Kaspersky Thin Client, Kaspersky Security Management Suite.
   - En el bloque **Estado de la directiva**, seleccione uno de los siguientes estados: *Activa*, *Inactiva* o *Fuera de la oficina*. El estado predeterminado es *Activa*.
   - Para definir si los ajustes de la directiva serán heredados, configure las siguientes opciones en el bloque **Herencia de configuración**:
     - Habilite o deshabilite la opción **Heredar configuración de la directiva primaria**.
     - Habilite o deshabilite la opción **Forzar la herencia de configuración en las directivas secundarias**.
5. Haga clic en el botón **Guardar** ubicado en la parte inferior de la página.

Se creará la directiva y se la mostrará en la lista de directivas de Web Console.

Modificar una directiva

Tras crear una directiva para un grupo de dispositivos con Kaspersky Thin Client, puede modificarla.

Para modificar una directiva:

1. En la ventana principal de Web Console, seleccione **Dispositivos → Directivas y perfiles**.
2. Seleccione la directiva que desee modificar.

3. Se abre una ventana para configurar la directiva. En la pestaña **General** de esta ventana, defina los siguientes ajustes:

   - Si necesita hacerlo, ingrese un nuevo nombre para la directiva en el campo **Nombre**.
   - Si desea cambiar el estado de la directiva, utilice el bloque **Estado de la directiva** para seleccionar uno de los siguientes estados: *Activa*, *Inactiva* o *Fuera de la oficina*.
   - Para definir si los ajustes de la directiva serán heredados, configure las siguientes opciones en el bloque **Herencia de configuración**:
     - Habilite o deshabilite la opción **Heredar configuración de la directiva primaria**.
     - Habilite o deshabilite la opción **Forzar la herencia de configuración en las directivas secundarias**.

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**.

Configurar Kaspersky Thin Client a través de Web Console

En esta sección, encontrará información para configurar los ajustes de Kaspersky Thin Client a través de Web Console.

Configurar los ajustes básicos de Kaspersky Thin Client a través de Web Console

Puede utilizar Web Console para configurar los ajustes generales de un dispositivo puntual o de un grupo de dispositivos que ejecuten Kaspersky Thin Client.

Cómo configurar los ajustes básicos de un dispositivo

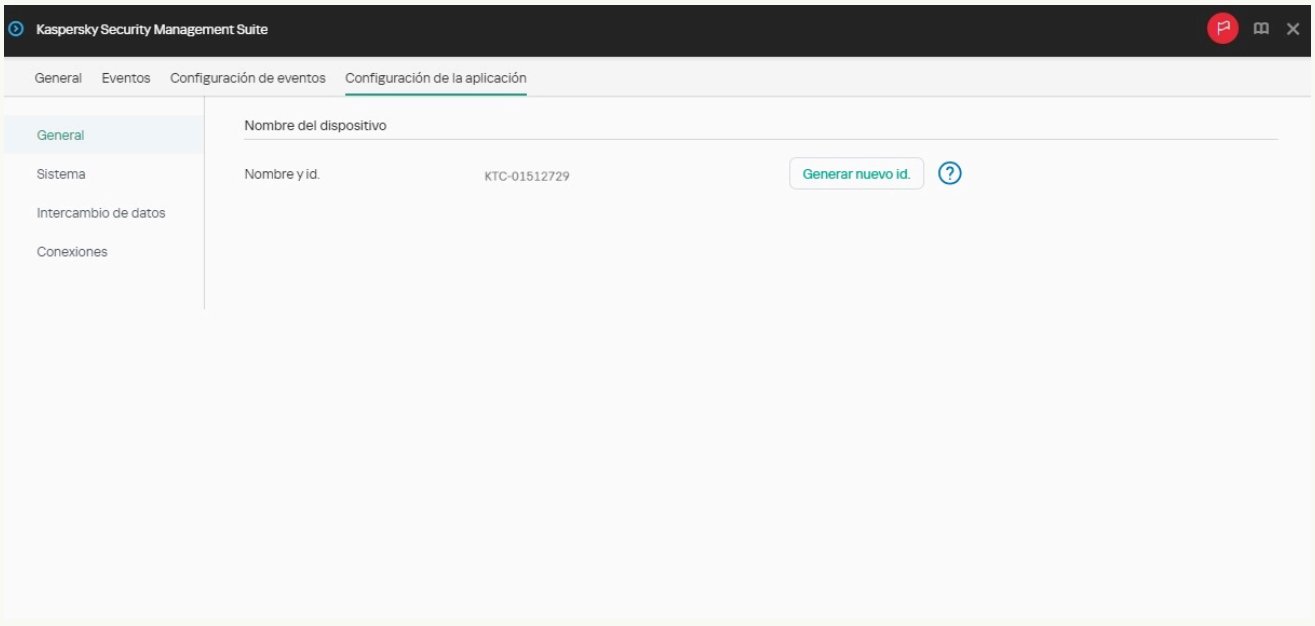
1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del cliente ligero en el que se esté ejecutando Kaspersky Thin Client. Encontrará el nombre del dispositivo en la interfaz de Kaspersky Thin Client. Si no ve el nombre del cliente ligero en la lista, agregue el dispositivo al grupo **Dispositivos administrados**.

   Si el dispositivo administrado forma parte de un grupo de administración y se ha impuesto una directiva que afecte los ajustes de ese grupo, no se aplicarán los ajustes que configure individualmente para el dispositivo.

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).



Ventana para configurar los ajustes generales de un dispositivo a través de Web Console

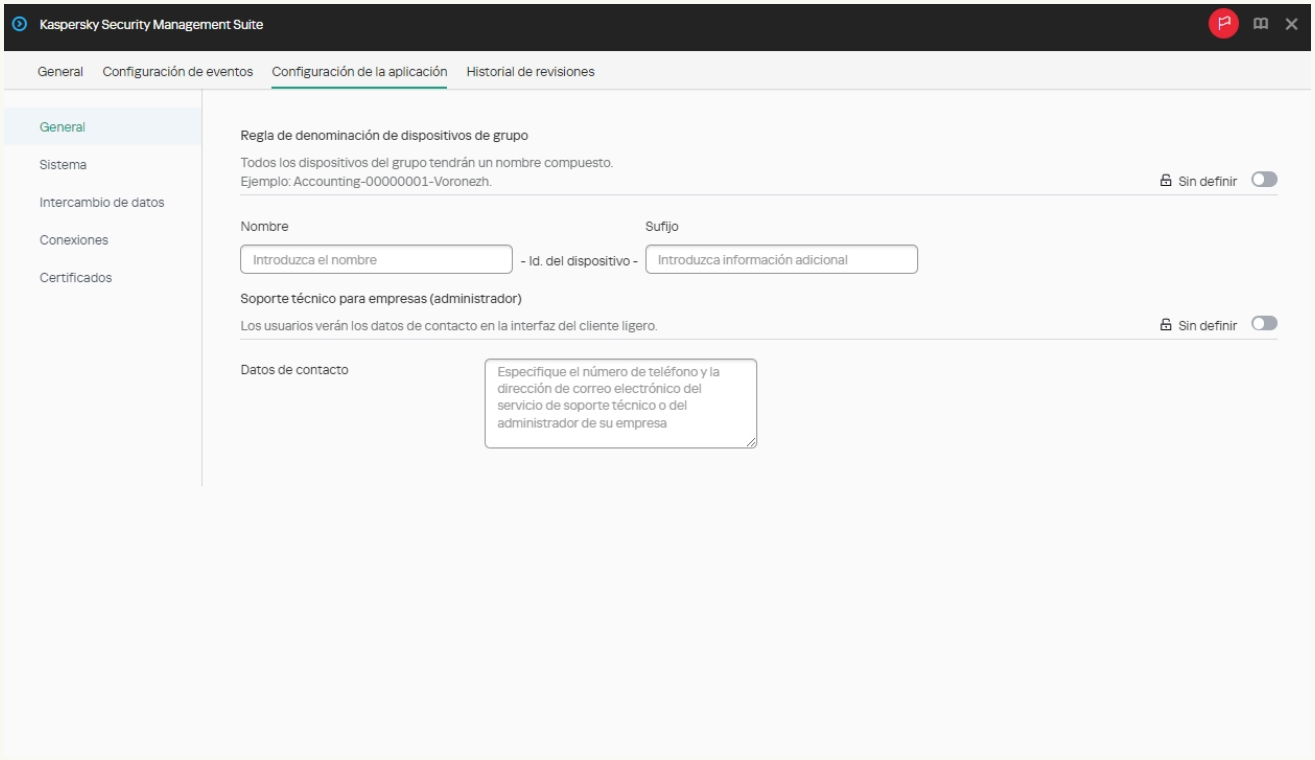
7. Si desea cambiar el id. incluido en el nombre del cliente ligero, haga clic en el botón **Generar nuevo id.** en el bloque **Nombre del dispositivo**. Para generar un nuevo identificador, el dispositivo administrado debe formar parte de un grupo de administración que tenga configurada e impuesta una directiva para una regla de denominación de dispositivos de grupo.

   El nuevo id. incluido en el nombre del cliente ligero se creará cuando el dispositivo se sincronice con Kaspersky Security Center.

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

Cómo configurar los ajustes básicos de un grupo de dispositivos

1. En la ventana principal de Web Console, seleccione **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).



Ventana para configurar los ajustes generales de un grupo de dispositivos a través de Web Console

5. Si desea definir un nuevo formato de nombre para los dispositivos del grupo de administración, en el bloque **Regla de denominación de dispositivos de grupo**, indique el nuevo nombre del grupo y la información adicional. Puede usar letras mayúsculas y minúsculas de los alfabetos latino y cirílico, como también caracteres especiales. Se generará automáticamente un identificador único (de ocho caracteres) para cada dispositivo del grupo. El nombre de un dispositivo no puede tener más de treinta caracteres.
6. Ponga el interruptor ubicado en el lado derecho del bloque **Regla de denominación de dispositivos de grupo** en la posición **Imponer**.

Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Imponer** (Imponer), los valores definidos para esos ajustes se hacen cumplir en los dispositivos que están sujetos a la directiva correspondiente. Tales ajustes no se pueden modificar a través de la interfaz de Kaspersky Thin Client. Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Sin definir** (Sin definir), los valores definidos para esos ajustes no se hacen cumplir en los dispositivos sujetos a la directiva correspondiente. Los valores de esos ajustes se pueden modificar en la interfaz de Kaspersky Thin Client y, si se trata de dispositivos administrados, en la sección **Dispositivos** → **Dispositivos administrados** de Web Console.

7. Agregue los datos de contacto del administrador de Kaspersky Security Center en el campo **Datos de contacto**. Puede ingresar el apellido, el nombre, el número de teléfono y la dirección de correo electrónico del administrador. El campo admite un máximo de ochenta caracteres.

   El usuario podrá ver los datos de contacto del administrador de Kaspersky Security Center en la ventana principal de Kaspersky Thin Client, en la ventana para confirmar el restablecimiento de los ajustes y datos de Kaspersky Thin Client, en la ventana para confirmar los cambios en los ajustes de conexión a Kaspersky Security Center y cuando se sustituya el certificado para conectarse a Kaspersky Security Center.

8. Ponga el interruptor ubicado en el lado derecho del bloque **Soporte técnico para empresas (administrador)** en la posición **Imponer**.

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

Configurar la conexión a un entorno remoto de Basis.WorkPlace a través de Web Console

A través de Web Console, puede configurar los ajustes que se usarán en un dispositivo o en un grupo de dispositivos con Kaspersky Thin Client para conectarse a un entorno remoto implementado en una infraestructura de Basis.WorkPlace.

Si desea ver instrucciones para conectarse a un entorno remoto, consulte este otro artículo.

Cómo configurar los ajustes para conectarse a un entorno remoto de Basis.WorkPlace para un dispositivo

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del cliente ligero en el que se esté ejecutando Kaspersky Thin Client. Encontrará el nombre del dispositivo en la interfaz de Kaspersky Thin Client. Si no ve el nombre del cliente ligero en la lista, agregue el dispositivo al grupo **Dispositivos administrados**.

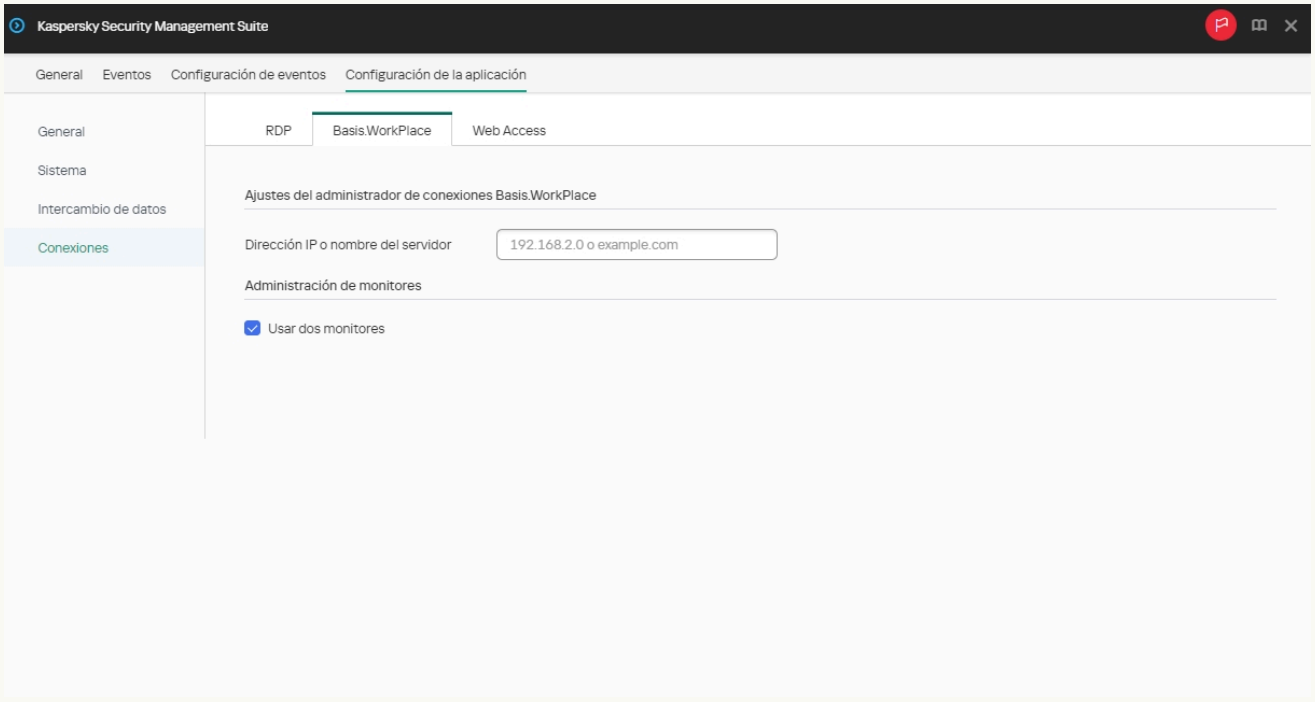
   Si el dispositivo administrado forma parte de un grupo de administración y se ha impuesto una directiva que afecte los ajustes de ese grupo, no se aplicarán los ajustes que configure individualmente para el dispositivo.

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 en la que puede configurar los ajustes que se usarán para conectarse a un entorno remoto de Basis.WorkPlace (vea la siguiente imagen).



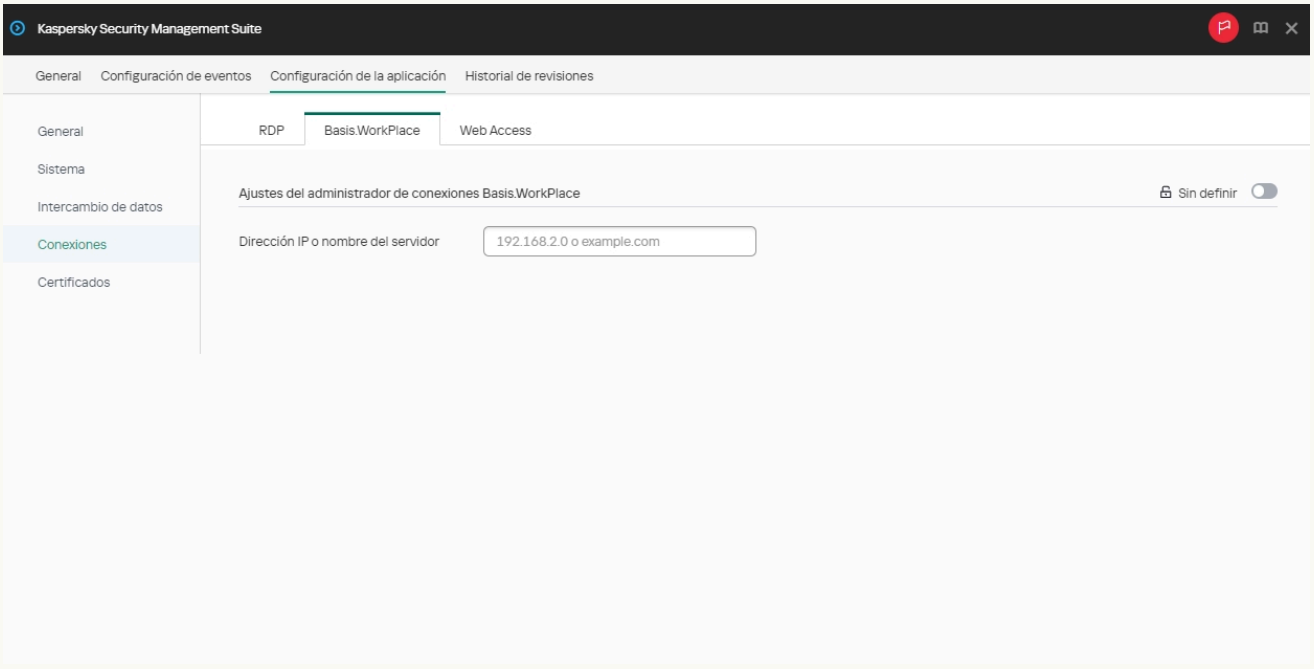
Ventana para configurar mediante Web Console los ajustes que se usarán en un dispositivo para conectarse a un escritorio remoto administrado por Basis.WorkPlace

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

Cómo configurar los ajustes para conectarse a un entorno remoto de Basis.WorkPlace para un grupo de dispositivos

1. En la ventana principal de Web Console, seleccione **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 en la que puede configurar los ajustes que se usarán para conectarse a un escritorio remoto administrado por Basis.WorkPlace (vea la siguiente imagen).



Ventana para configurar mediante Web Console los ajustes que se usarán en un grupo de dispositivos para conectarse a un escritorio remoto administrado por Basis.WorkPlace

5. En **Dirección IP o nombre del servidor**, ingrese la dirección IP o el nombre del servidor al que desee conectarse.
6. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.

Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Imponer** (Imponer), los valores definidos para esos ajustes se hacen cumplir en los dispositivos que están sujetos a la directiva correspondiente. Tales ajustes no se pueden modificar a través de la interfaz de Kaspersky Thin Client. Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Sin definir** (Sin definir), los valores definidos para esos ajustes no se hacen cumplir en los dispositivos sujetos a la directiva correspondiente. Los valores de esos ajustes se pueden modificar en la interfaz de Kaspersky Thin Client y, si se trata de dispositivos administrados, en la sección **Dispositivos** → **Dispositivos administrados** de Web Console.

Cuando se trabaja con Kaspersky Thin Client a través de Basis.WorkPlace, rigen las siguientes limitaciones:

- No se pueden utilizar tarjetas inteligentes para autorizar a los usuarios en el administrador de conexiones de Basis.WorkPlace.
- Los usuarios no pueden iniciar un cambio de contraseña en Kaspersky Thin Client.
- No es posible conectarse simultáneamente a más de un escritorio remoto administrado por Basis.WorkPlace.

Configurar una conexión RDP a un entorno remoto a través de Web Console

A través de Web Console, puede configurar los ajustes que se usarán en un dispositivo o en un grupo de dispositivos con Kaspersky Thin Client para conectarse a un escritorio remoto o a un entorno virtual mediante el protocolo RDP.

Si desea ver instrucciones para conectarse a un entorno remoto, consulte este otro artículo.

Cómo configurar los ajustes para conectarse a un entorno remoto a través de RDP para un dispositivo

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del cliente ligero en el que se esté ejecutando Kaspersky Thin Client. Encontrará el nombre del dispositivo en la interfaz de Kaspersky Thin Client. Si no ve el nombre del cliente ligero en la lista, agregue el dispositivo al grupo **Dispositivos administrados**.

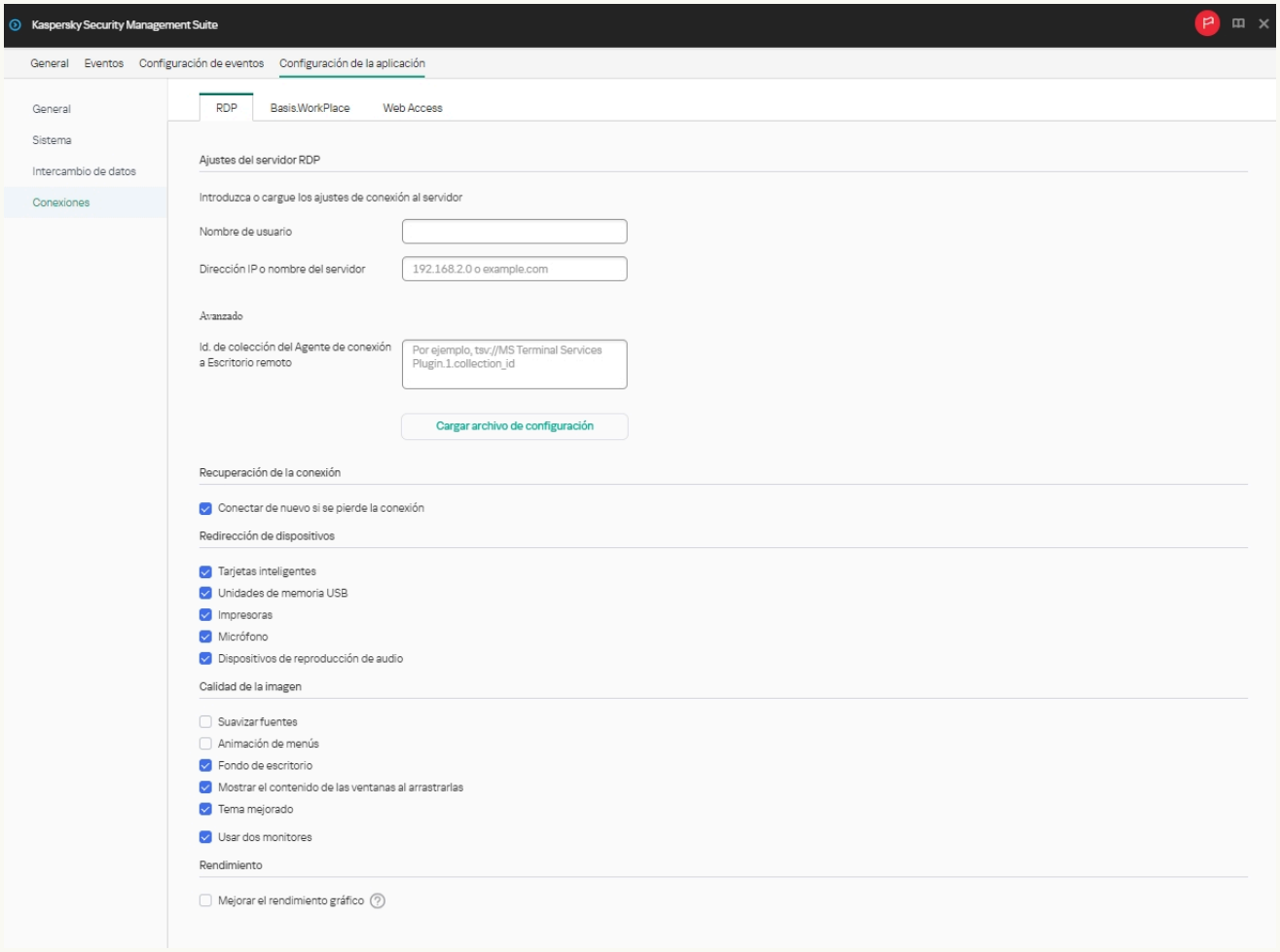
   Si el dispositivo administrado forma parte de un grupo de administración y se ha impuesto una directiva que afecte los ajustes de ese grupo, no se aplicarán los ajustes que configure individualmente para el dispositivo.

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 en la que puede configurar los ajustes que se usarán para conectarse a un escritorio remoto o a una aplicación virtual a través de RDP (vea la siguiente imagen).



Ventana para configurar mediante Web Console los ajustes que se usarán en un dispositivo para conectarse a un escritorio remoto por RDP

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

8. En el campo **Nombre de usuario**, ingrese el nombre de la cuenta de usuario con la que se establecerá la conexión.

9. 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).

   Ingrese un identificador de colección del Agente de conexión a Escritorio remoto para conectarse a una aplicación virtual.

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

    Ingrese un identificador de colección del Agente de conexión a Escritorio remoto para conectarse a una aplicación virtual.

    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 **Aplicación**.

11. Si desea que la conexión se restablezca automáticamente ante una desconexión inesperada, marque la casilla **Conectar de nuevo si se pierde la conexión**.

12. En el bloque **Redirección de dispositivos**, marque las casillas adyacentes a los dispositivos que corresponda:

    - Marque **Tarjetas inteligentes** si desea habilitar la redirección de tarjetas inteligentes y tókenes.
    - Marque **Unidades de memoria USB** si desea habilitar la redirección de unidades de memoria USB.
    - Marque **Impresoras** si desea habilitar la redirección de impresoras.

      La computadora remota deberá tener instalado el controlador de la impresora conectada al cliente ligero.
    - **Micrófono** si desea habilitar la redirección de dispositivos de grabación de audio.

      El volumen de audio y otras configuraciones se administran desde el equipo remoto.
    - **Dispositivos de reproducción de audio** si desea habilitar la redirección de auriculares o altavoces.

      Kaspersky Thin Client puede reproducir audio mono y estéreo. El volumen del audio y otros ajustes se controlan desde el entorno remoto.

13. En el bloque **Calidad de la imagen**, marque las casillas ubicadas junto a los ajustes de gráficos del escritorio remoto que desee 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.

14. 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**.

15. Para mejorar el rendimiento cuando se conecte a aplicaciones o escritorios remotos, en el bloque **Rendimiento**, marque **Mejorar el rendimiento gráfico**.

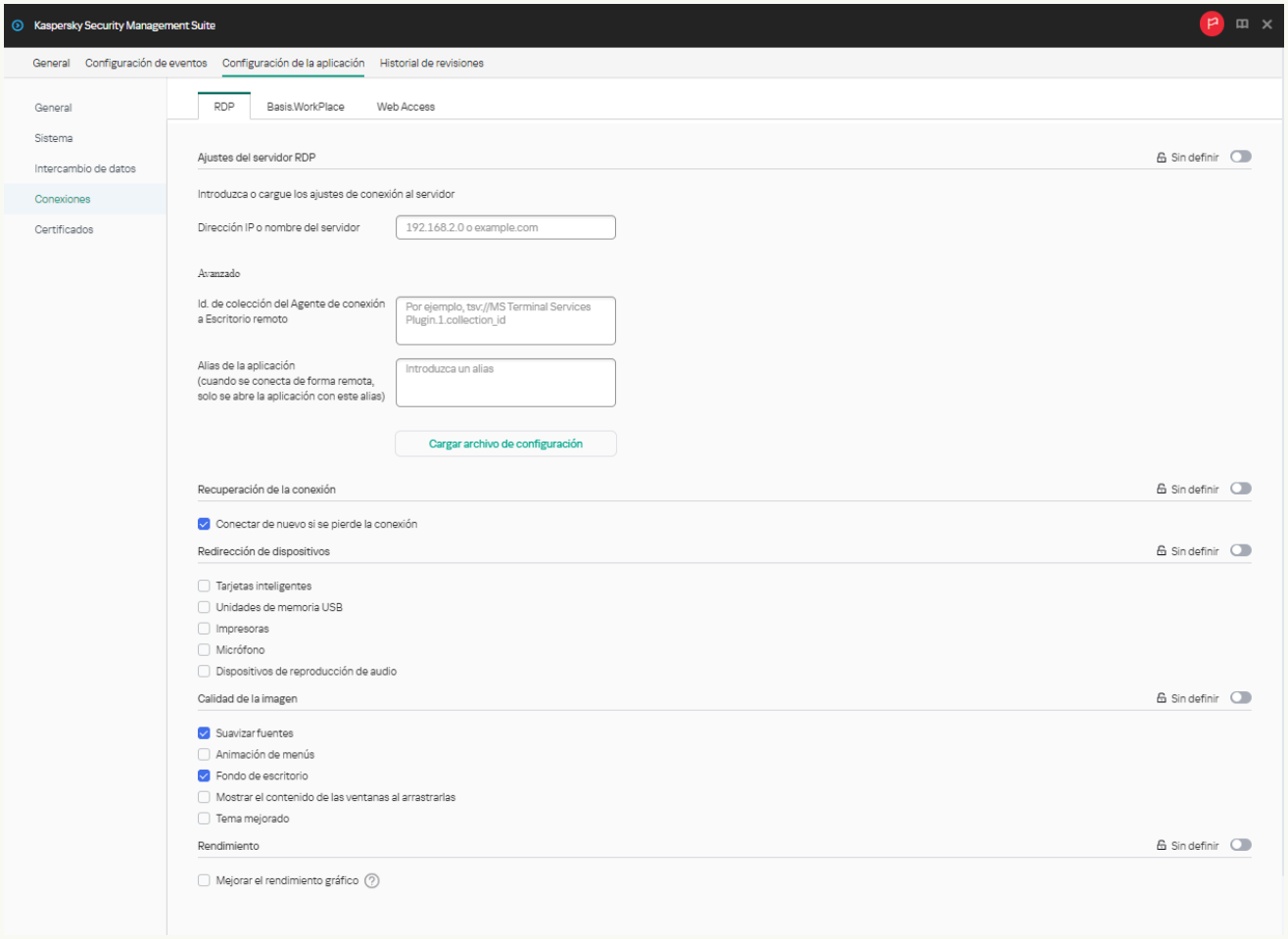
    Si el usuario necesita conectarse a un escritorio remoto de Microsoft Windows 7, desmarque **Mejorar el rendimiento gráfico**. La función no es compatible con las conexiones a escritorios remotos que ejecuten Microsoft Windows 7.

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

Cómo configurar los ajustes para conectarse a un entorno remoto a través de RDP para un grupo de dispositivos

1. En la ventana principal de Web Console, seleccione **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 en la que puede configurar los ajustes que se usarán para conectarse a un escritorio remoto a través de RDP (vea la siguiente imagen).



Ventana para configurar mediante Web Console los ajustes que se usarán en un grupo de dispositivos para conectarse a un escritorio remoto por RDP

5. En el campo **Servidor**, ingrese la dirección IP o el nombre del servidor que desee usar para conectarse a un escritorio remoto a través de RDP.
6. En el campo **Nombre de usuario**, ingrese el nombre de la cuenta de usuario que se usará para conectarse al escritorio remoto a través de RDP.

7. 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).

   Ingrese un identificador de colección del Agente de conexión a Escritorio remoto para conectarse a una aplicación virtual.

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

   Especifique un id. de colección del Agente de conexión a escritorio remoto para conectarse a una aplicación remota.

   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 **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. En el bloque **Redirección de dispositivos**, marque las casillas adyacentes a los dispositivos que corresponda:

    - Marque **Tarjetas inteligentes** si desea habilitar la redirección de tarjetas inteligentes y tókenes.
    - Marque **Unidades de memoria USB** si desea habilitar la redirección de unidades de memoria USB.
    - Marque **Impresoras** si desea habilitar la redirección de impresoras.

      La computadora remota deberá tener instalado el controlador de la impresora conectada al cliente ligero.

    - **Micrófono** si desea habilitar la redirección de dispositivos de grabación de audio.

      El volumen de audio y otras configuraciones se administran desde el equipo remoto.

    - **Dispositivos de reproducción de audio** si desea habilitar la redirección de auriculares o altavoces.

      Kaspersky Thin Client puede reproducir audio mono y estéreo. El volumen del audio y otros ajustes se controlan desde el entorno remoto.

11. En el bloque **Calidad de la imagen**, marque las casillas ubicadas junto a los ajustes de gráficos del escritorio remoto que desee 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.

12. Para mejorar el rendimiento cuando se conecte a aplicaciones o escritorios remotos, en el bloque **Rendimiento**, marque **Mejorar el rendimiento gráfico**.

    Si el usuario necesita conectarse a un escritorio remoto de Microsoft Windows 7, desmarque **Mejorar el rendimiento gráfico**. La función no es compatible con las conexiones a escritorios remotos que ejecuten Microsoft Windows 7.

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

Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Imponer** (Imponer), los valores definidos para esos ajustes se hacen cumplir en los dispositivos que están sujetos a la directiva correspondiente. Tales ajustes no se pueden modificar a través de la interfaz de Kaspersky Thin Client. Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Sin definir** (Sin definir), los valores definidos para esos ajustes no se hacen cumplir en los dispositivos sujetos a la directiva correspondiente. Los valores de esos ajustes se pueden modificar en la interfaz de Kaspersky Thin Client y, si se trata de dispositivos administrados, en la sección **Dispositivos** → **Dispositivos administrados** de Web Console.

Configurar la conexión a un entorno remoto disponible en Web Access a través de Web Console

A través de Web Console, puede configurar los ajustes que se usarán en un dispositivo o en un grupo de dispositivos con Kaspersky Thin Client para conectarse 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 y VMware Horizon. Web Access admite HTML5 y proporciona una conexión HTTPS segura al conectarse.

Si desea ver instrucciones para conectarse a un entorno remoto, consulte este otro artículo.

Cómo configurar los ajustes para conectarse a un entorno remoto en Web Access para un dispositivo

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del cliente ligero en el que se esté ejecutando Kaspersky Thin Client. Encontrará el nombre del dispositivo en la interfaz de Kaspersky Thin Client. Si no ve el nombre del cliente ligero en la lista, agregue el dispositivo al grupo **Dispositivos administrados**.

   Si el dispositivo administrado forma parte de un grupo de administración y se ha impuesto una directiva que afecte los ajustes de ese grupo, no se aplicarán los ajustes que configure individualmente para el dispositivo.

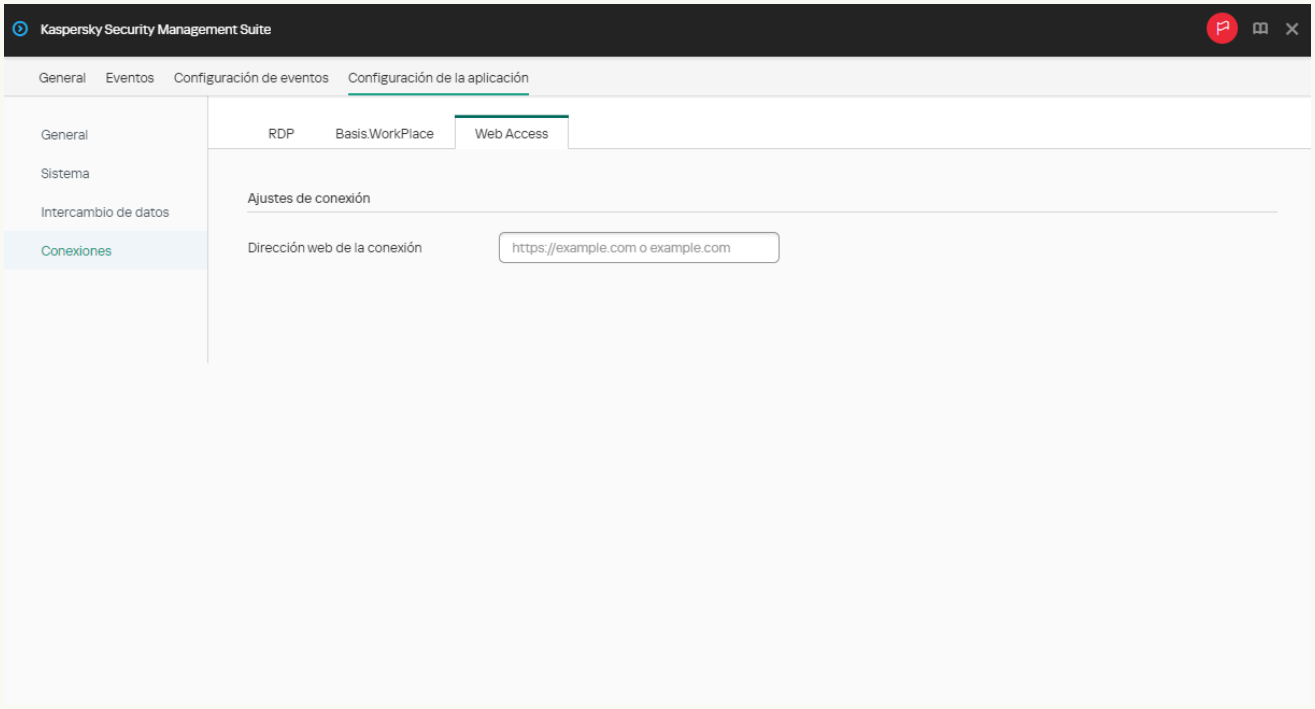
3. En la ventana que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre del complemento web Kaspersky Security Management Suite.

   Se abre una ventana con información sobre Kaspersky Thin Client.

5. Seleccione la pestaña **Configuración de la aplicación**.

   Seleccione **Conexiones** → **Web Access**.

   Se abre la ventana para configurar los ajustes de conexión (vea la siguiente imagen).



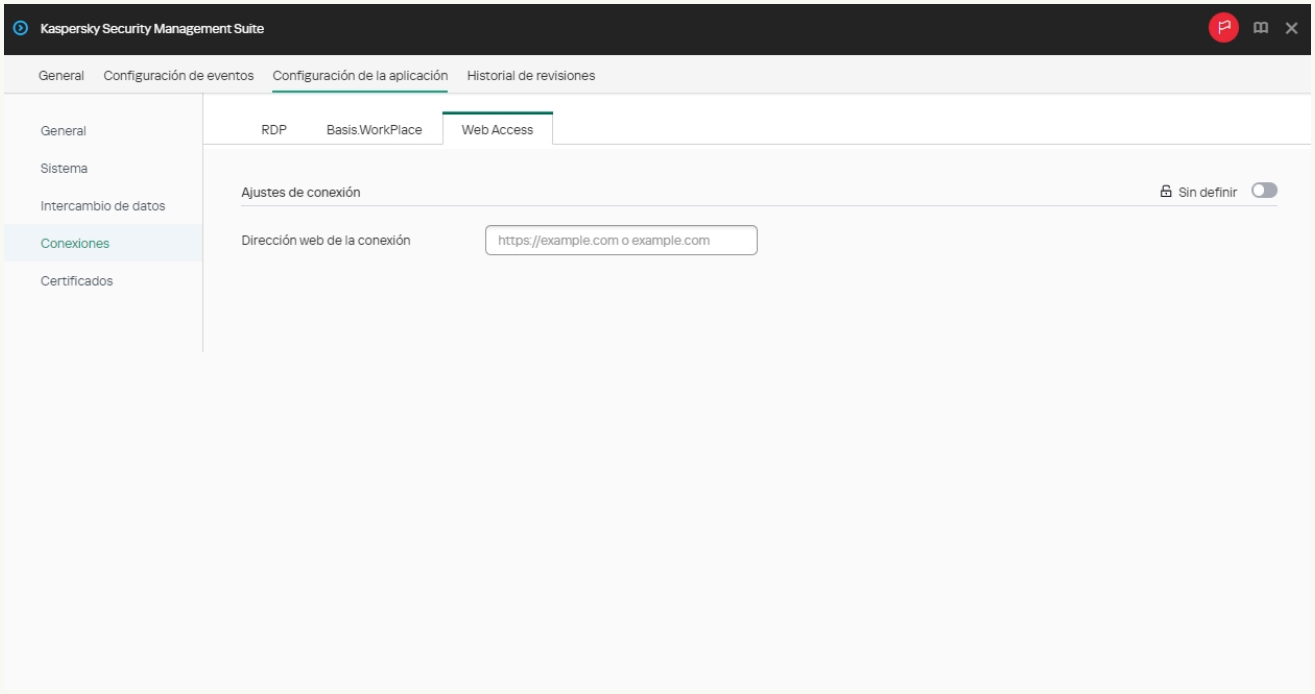
Ventana de configuración para conectarse a un entorno en Web Access a través de Web Console

6. En el campo **Dirección web de la conexión**, ingrese la dirección web del servidor que se usará para conectarse al entorno remoto.
7. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.

[Cómo configurar los ajustes para conectarse a un entorno remoto en Web Access para un grupo de dispositivos]

1. En la ventana principal de Web Console, seleccione **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 la ventana para configurar los ajustes de conexión (vea la siguiente imagen).



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

5. En el campo **Dirección web de la conexión**, ingrese la dirección web del servidor que se usará para conectarse al entorno remoto.
6. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.

La compatibilidad de Kaspersky Thin Client con los escritorios remotos de Citrix Workspace tiene las siguientes limitaciones:

- No se admite el uso compartido de archivos entre el cliente ligero y el escritorio remoto.
- No se admite el uso compartido del portapapeles entre el cliente ligero y el escritorio remoto.
- No se admite la redirección de unidades de memoria USB, tarjetas inteligentes y tókenes USB.

Configurar los ajustes de ahorro de energía de Kaspersky Thin Client a través de Web Console

Puede utilizar Web Console para configurar los ajustes de ahorro de energía para un dispositivo o para un grupo de dispositivos que ejecuten Kaspersky Thin Client.

Cómo configurar los ajustes de ahorro de energía para un dispositivo

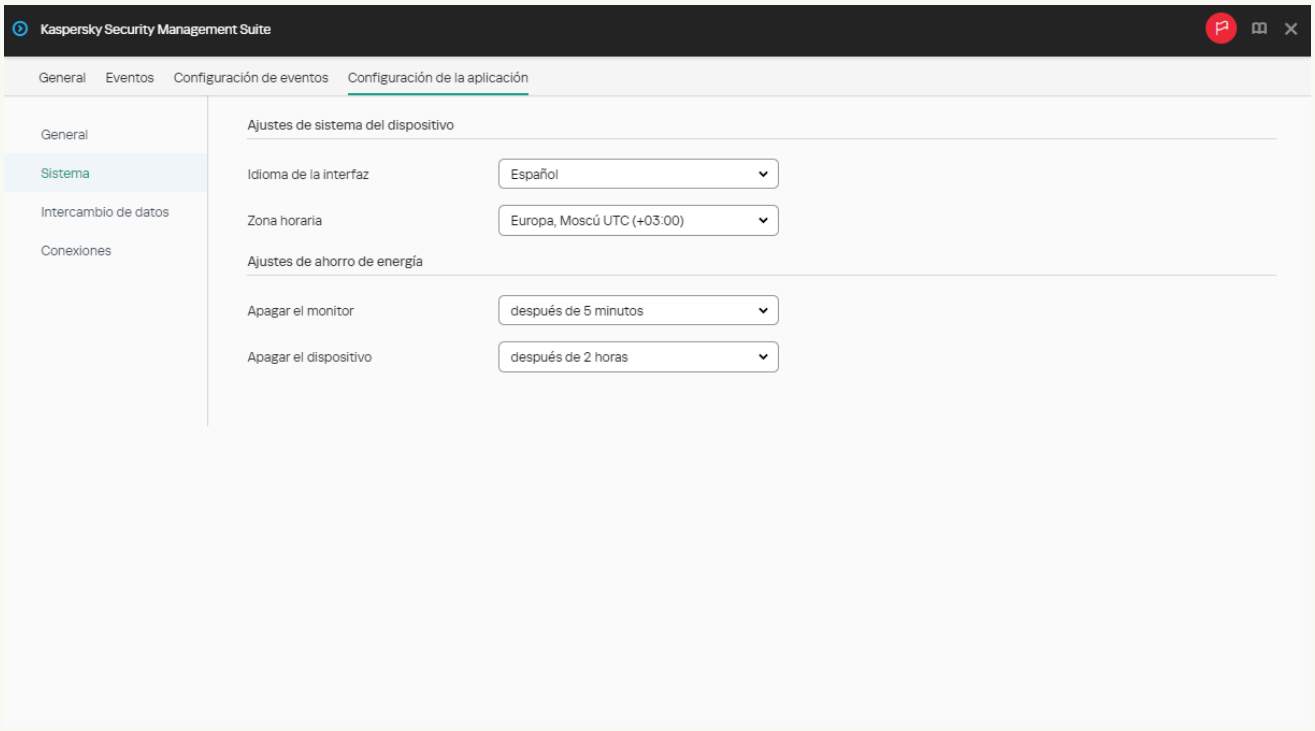
1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del cliente ligero en el que se esté ejecutando Kaspersky Thin Client. Encontrará el nombre del dispositivo en la interfaz de Kaspersky Thin Client. Si no ve el nombre del cliente ligero en la lista, agregue el dispositivo al grupo **Dispositivos administrados**.

   Si el dispositivo administrado forma parte de un grupo de administración y se ha impuesto una directiva que afecte los ajustes de ese grupo, no se aplicarán los ajustes que configure individualmente para el dispositivo.

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).



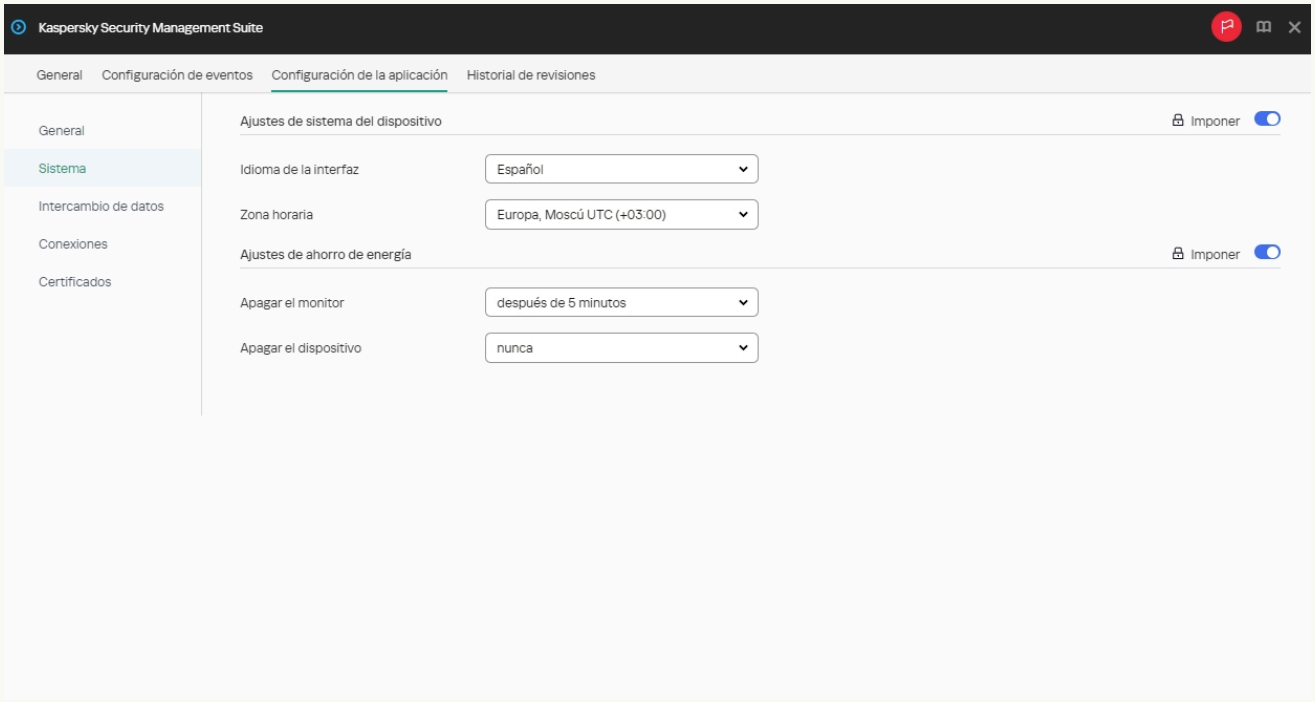
Ventana para configurar los ajustes de ahorro de energía para un dispositivo a través de Web Console

7. 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.
8. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.

Luego de que Kaspersky Thin Client se sincronice con Kaspersky Security Center, los ajustes de ahorro de energía se aplicarán a Kaspersky Thin Client.

Cómo configurar los ajustes de ahorro de energía para un grupo de dispositivos

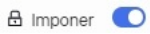
1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Sistema** (vea la siguiente imagen).



Ventana para configurar los ajustes de ahorro de energía para un grupo de dispositivos a través de Web Console

5. 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.
6. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.

Una vez que todos los dispositivos del grupo de administración se sincronicen con Kaspersky Security Center, los ajustes de ahorro de energía se aplicarán a todos los dispositivos con Kaspersky Thin Client que formen parte del grupo.

Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Imponer** (

), los valores definidos para esos ajustes se hacen cumplir en los dispositivos que están sujetos a la directiva correspondiente. Tales ajustes no se pueden modificar a través de la interfaz de Kaspersky Thin Client. Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Sin definir** (

), los valores definidos para esos ajustes no se hacen cumplir en los dispositivos sujetos a la directiva correspondiente. Los valores de esos ajustes se pueden modificar en la interfaz de Kaspersky Thin Client y, si se trata de dispositivos administrados, en la sección **Dispositivos** → **Dispositivos administrados** de Web Console.

Configurar el idioma de la interfaz y la zona horaria de Kaspersky Thin Client a través de Web Console

Puede utilizar Web Console para configurar el idioma de la interfaz y la zona horaria de un dispositivo o de un grupo de dispositivos que ejecuten Kaspersky Thin Client.

Cómo configurar el idioma de la interfaz y la zona horaria de un dispositivo

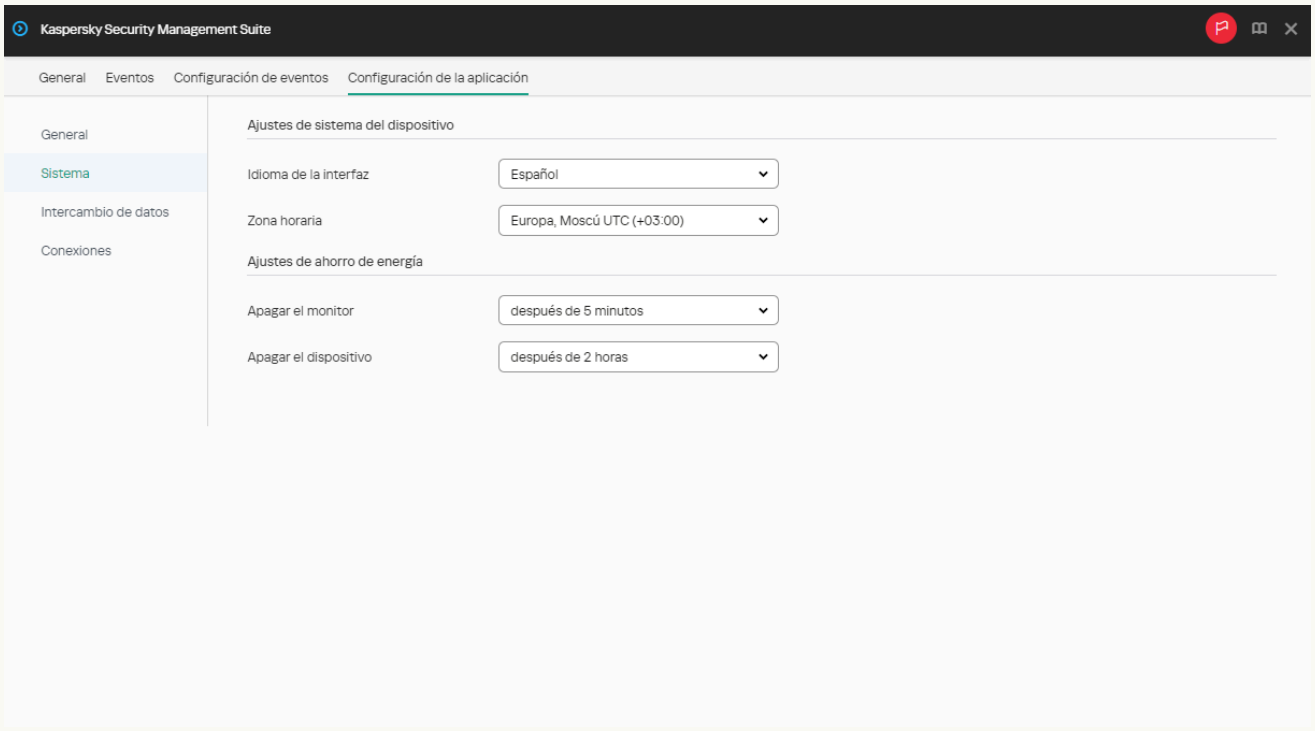
1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del cliente ligero en el que se esté ejecutando Kaspersky Thin Client. Encontrará el nombre del dispositivo en la interfaz de Kaspersky Thin Client. Si no ve el nombre del cliente ligero en la lista, agregue el dispositivo al grupo **Dispositivos administrados**.

   Si el dispositivo administrado forma parte de un grupo de administración y se ha impuesto una directiva que afecte los ajustes de ese grupo, no se aplicarán los ajustes que configure individualmente para el dispositivo.

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).

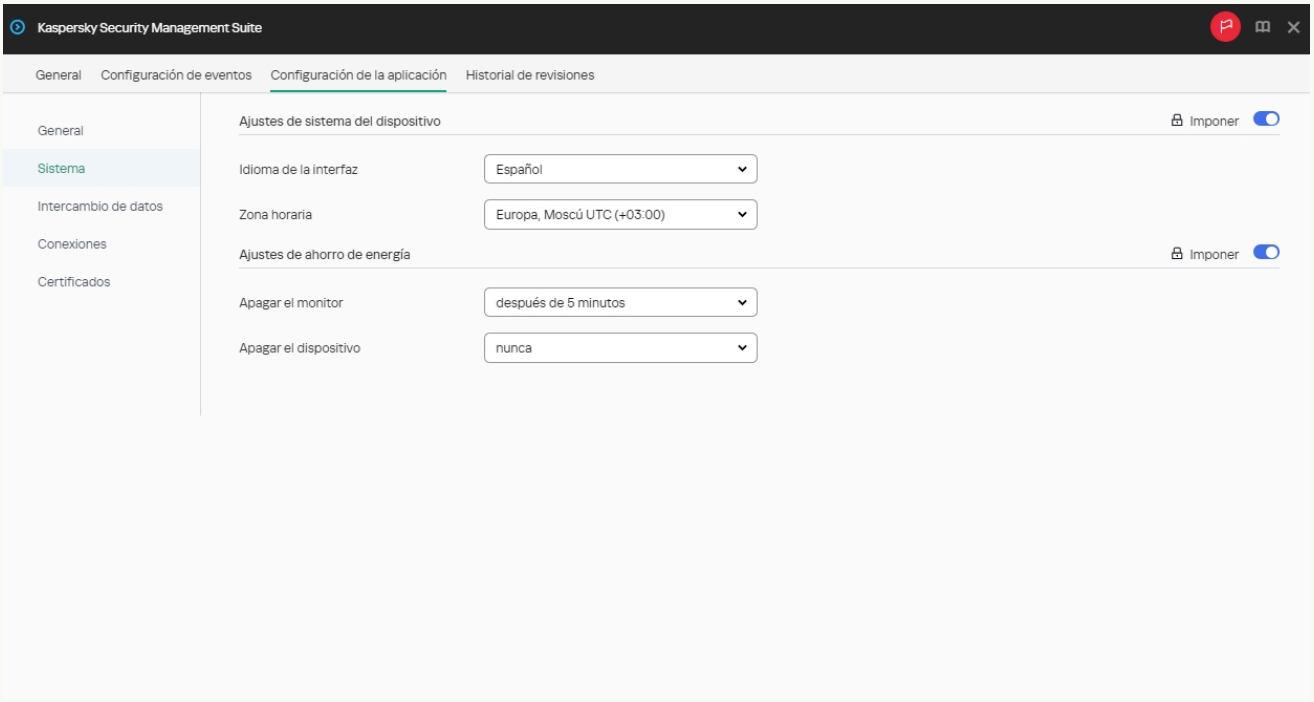


Ventana para configurar el idioma de la interfaz y la zona horaria a través de Web Console para un dispositivo

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

Cómo configurar el idioma de la interfaz y la zona horaria de un grupo de dispositivos

1. En la ventana principal de Web Console, seleccione **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 el idioma de la interfaz y la zona horaria a través de Web Console para un grupo de dispositivos

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

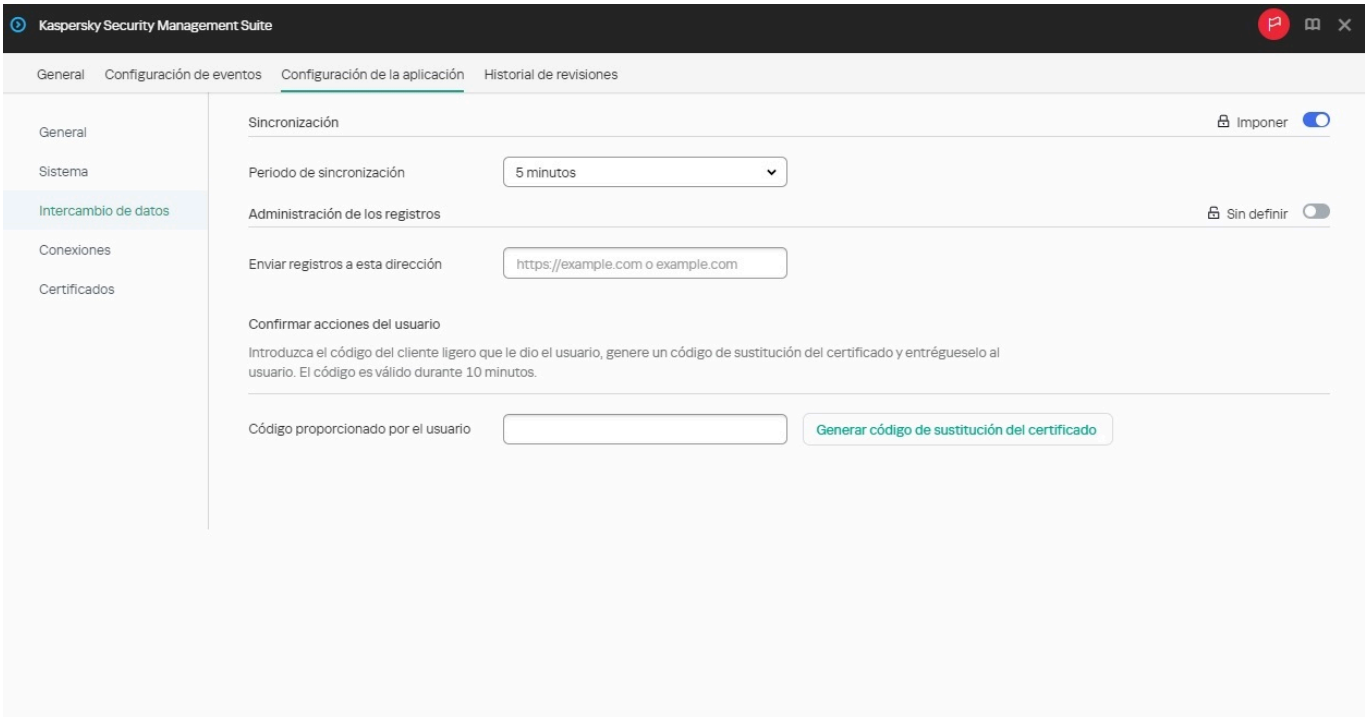
Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Imponer** (Imponer), los valores definidos para esos ajustes se hacen cumplir en los dispositivos que están sujetos a la directiva correspondiente. Tales ajustes no se pueden modificar a través de la interfaz de Kaspersky Thin Client. Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Sin definir** (Sin definir), los valores definidos para esos ajustes no se hacen cumplir en los dispositivos sujetos a la directiva correspondiente. Los valores de esos ajustes se pueden modificar en la interfaz de Kaspersky Thin Client y, si se trata de dispositivos administrados, en la sección **Dispositivos** → **Dispositivos administrados** de Web Console.

Configurar la sincronización entre Kaspersky Thin Client y Kaspersky Security Center

A través de Web Console, puede configurar la sincronización con Kaspersky Security Center solo para un grupo de dispositivos que ejecuten Kaspersky Thin Client.

Para configurar la sincronización entre Kaspersky Thin Client y Kaspersky Security Center:

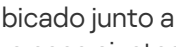
1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva del complemento web Kaspersky Security Management Suite.
3. En la ventana que se abre, seleccione la pestaña **Configuración de la aplicación**.
4. Elija la sección **Intercambio de datos** (vea la siguiente imagen).

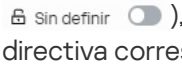


Ventana para configurar la sincronización entre Kaspersky Thin Client y Kaspersky Security Center

5. En el campo **Periodo de sincronización**, defina la frecuencia con la que se realizará la sincronización entre Kaspersky Thin Client y Kaspersky Security Center.

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

Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Imponer** (

), los valores definidos para esos ajustes se hacen cumplir en los dispositivos que están sujetos a la directiva correspondiente. Tales ajustes no se pueden modificar a través de la interfaz de Kaspersky Thin Client. Cuando el interruptor ubicado junto a un grupo de ajustes se encuentra en la posición **Sin definir** (

), los valores definidos para esos ajustes no se hacen cumplir en los dispositivos sujetos a la directiva correspondiente. Los valores de esos ajustes se pueden modificar en la interfaz de Kaspersky Thin Client y, si se trata de dispositivos administrados, en la sección **Dispositivos** → **Dispositivos administrados** de Web Console.

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

A través de Web Console, puede configurar el envío de los registros de Kaspersky Thin Client a un servidor de registros para un dispositivo o para un grupo de dispositivos que ejecuten Kaspersky Thin Client.

Cómo configurar el envío de registros para un dispositivo

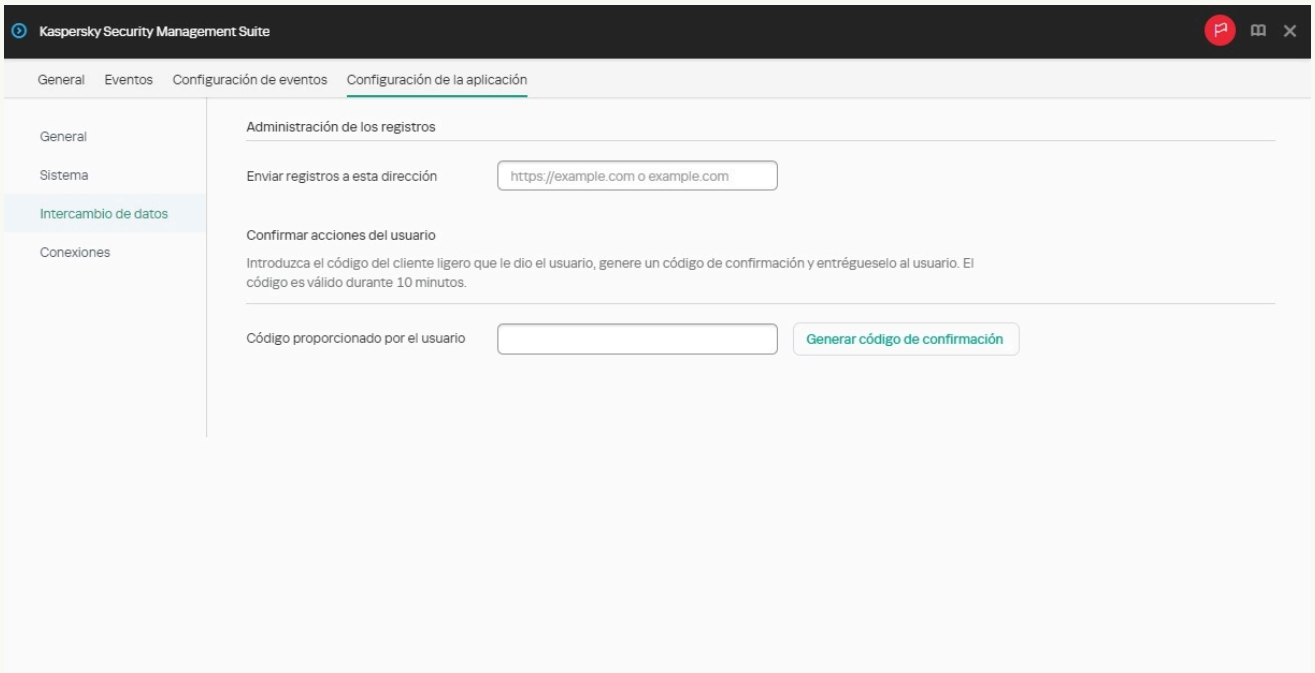
1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del cliente ligero en el que se esté ejecutando Kaspersky Thin Client. Encontrará el nombre del dispositivo en la interfaz de Kaspersky Thin Client. Si no ve el nombre del cliente ligero en la lista, agregue el dispositivo al grupo **Dispositivos administrados**.

   Si el dispositivo administrado forma parte de un grupo de administración y se ha impuesto una directiva que afecte los ajustes de ese grupo, no se aplicarán los ajustes que configure individualmente para el dispositivo.

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).

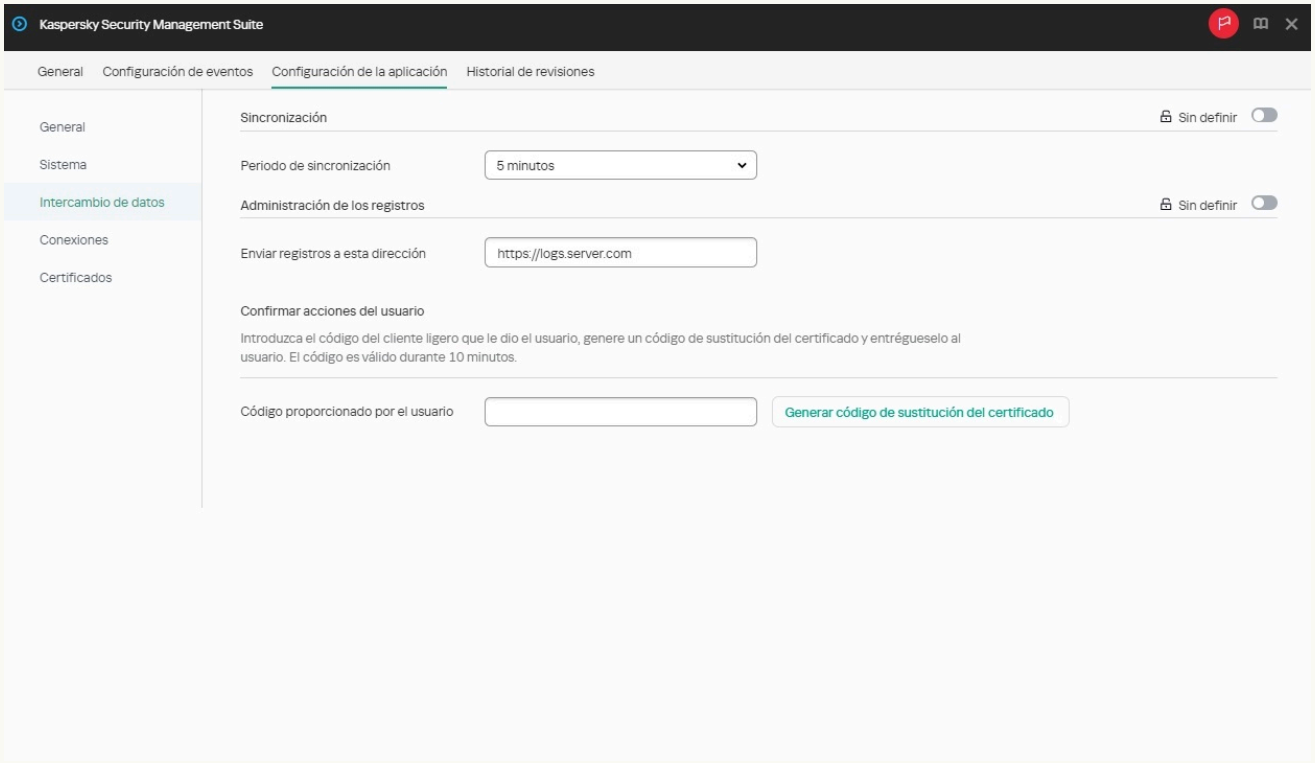


Ventana para configurar el envío de los registros de Kaspersky Thin Client para un dispositivo a través de Web Console

7. En el campo **Enviar registros a esta dirección**, ingrese la dirección del servidor de registros de destino en formato https://<dirección del servidor>. Asegúrese de que exista un servidor de registros que cumpla con los requisitos en la infraestructura de su empresa.
8. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.

Cómo configurar el envío de registros para un grupo de dispositivos

1. En la ventana principal de Web Console, seleccione **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 a través de Web Console para un grupo de dispositivos

5. En el campo **Enviar registros a esta dirección**, ingrese la dirección del servidor de registros de destino en formato https://<dirección del servidor>. Asegúrese de que exista un servidor de registros que cumpla con los requisitos en la infraestructura de su empresa.
6. Haga clic en **Guardar** en la parte inferior de la ventana para guardar los cambios.

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 se ha conectado a Kaspersky Security Center (o si se lo ha conectado, pero no se lo ha incluido en el grupo de dispositivos administrados), las solicitudes para confirmar las acciones enumeradas arriba no se enviarán al administrador. Agregue el cliente ligero al grupo de dispositivos administrados a fin de que el administrador reciba las solicitudes de confirmación para las acciones de los usuarios.

Para confirmar las modificaciones en los ajustes de conexión a Kaspersky Security Center o el restablecimiento de todos los ajustes del cliente ligero:

1. En la ventana principal de Web Console, seleccione **Dispositivos** → **Dispositivos administrados**.
2. Haga clic en el nombre del cliente ligero en el que se esté ejecutando Kaspersky Thin Client. Encontrará el nombre del dispositivo en la interfaz de Kaspersky Thin Client. Si no ve el nombre del cliente ligero en la lista, agregue el dispositivo al grupo **Dispositivos administrados**.

   Si el dispositivo administrado forma parte de un grupo de administración y se ha impuesto una directiva que afecte los ajustes de ese grupo, no se aplicarán los ajustes que configure individualmente para el dispositivo.

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 **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.

Se recomienda configurar la conexión de un grupo de clientes ligeros a un servidor de registro o a un entorno remoto utilizando únicamente los certificados asignados por el administrador en Web Console. 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 sección *Acerca de los certificados* de 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 ícono ubicado junto al nombre del Servidor de administración de Kaspersky Security Center.

   Se abre la ventana **Propiedades del Servidor de administración**.

2. En la lista de subsecciones, elija **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 conectar Kaspersky Thin Client 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 de los certificados de Kaspersky Security Center indicados en la sección *Requisitos para los certificados personalizados que se utilizan en Kaspersky Security Center* de 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.

De ser necesario, puede convertir el archivo del certificado del formato PEM al formato DER.

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 administrados.

Recomendamos que se familiarice con los requisitos de los certificados de Kaspersky Security Center indicados en la sección *Requisitos para los certificados personalizados que se utilizan en Kaspersky Security Center* de 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 ícono ubicado junto al nombre del Servidor de administración de Kaspersky Security Center.

   Se abre la ventana **Propiedades del Servidor de administración**.
2. En la lista de subsecciones, elija **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:

   a. En la lista desplegable **Tipo de certificado**, seleccione **Certificado X.509**.

   b. Si el certificado de usuario está protegido con contraseña, ingrese la contraseña.

   c. Haga clic en el botón **Examinar** del bloque **Certificado** y seleccione el archivo del certificado de usuario.

   d. Haga clic en el botón **Examinar** del bloque **Clave privada** y seleccione la clave privada del certificado de usuario.

5. Haga clic en **Guardar** para guardar el certificado que desea agregar.

6. 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 administrados y 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

A través de Web Console, puede agregar certificados que permitan que los clientes ligeros de un grupo de administración se conecten a un entorno remoto o a un servidor de registros.

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 **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

Puede utilizar Web Console para eliminar los certificados de los clientes ligeros que formen parte de 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 **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 notificaciones en Kaspersky Security Center Web Console sobre los eventos registrados en Kaspersky Thin Client

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 gravedad. Dependiendo de las circunstancias en las que ocurre, a un evento se le puede asignar uno de los siguientes niveles de gravedad:

- 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 **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 gravedad de los eventos cuya información desee recibir:
   - **Crítico**
   - **Error funcional**
   - **Advertencia**
   - **Información**

   Aparece una tabla de eventos asociados al nivel de gravedad 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 gravedad especificada al Servidor de administración de Kaspersky Security Center. De manera predeterminada, los eventos se almacenan por treinta días.

[Cómo configurar las notificaciones de eventos para un grupo de dispositivos]

1. En la ventana principal de Web Console, seleccione **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 gravedad de los eventos cuya información desee recibir:
   - **Crítico**
   - **Error funcional**
   - **Advertencia**
   - **Información**

   Aparece una tabla de eventos asociados al nivel de gravedad 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 gravedad 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, vea la sección *Configurar el envío de notificaciones* en la guía de 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 **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 en el dispositivo.
- **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.
- **Nivel de gravedad**: muestra la gravedad del evento (*Crítico*, *Error funcional*, *Advertencia* o *Información*).
- **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 escritorio remoto.

Si no puede resolver el problema, comuníquese con Soporte técnico. De ser necesario, los especialistas en soporte técnico le pedirán que les envíe información del sistema o el registro de eventos.

Desconectarse de un escritorio remoto

Cuando Kaspersky Thin Client se desconecta de un escritorio remoto debido a un error, la conexión se restablece automáticamente si la opción para ello se encuentra habilitada en los ajustes de conexión al entorno remoto.

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 volver a trabajar con el escritorio remoto:

1. Cierre el mensaje de error.
2. Intente conectarse al escritorio remoto.
3. Si no puede establecer la conexión, reinicie el cliente ligero e intente conectarse al escritorio remoto nuevamente.
4. Si aun así no puede conectarse, comuníquese con el administrador de su empresa: Kaspersky Thin Client podría estar desconectándose del escritorio remoto debido a un problema físico.
5. Si se establece la conexión directa, pero aún no puede conectarse al escritorio remoto, comuníquese con Soporte técnico.

Probar la conexión de red

Para probar si el cliente ligero está conectado a la red:

Ver el estado de la conexión de red de Kaspersky Thin Client en el panel de control de Kaspersky Thin Client.

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. Aquí se almacena información sobre los certificados cargados en Kaspersky Thin Client e información sobre los casos en los que se utilizó Kaspersky Security Center para habilitar o deshabilitar la administración de los clientes ligeros. 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.

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 subproceso.
- Id. de la versión del producto.

El registro de auditoría de Kaspersky Thin Client contiene la siguiente información:

- Fecha y hora en que se cargó el certificado para conectar Kaspersky Thin Client a Kaspersky Security Center.
- Dirección del Servidor de administración de Kaspersky Security Center (dirección IP y/o nombre de dominio del servidor).
- Número de puerto del Servidor de administración de Kaspersky Security Center.
- 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, id. del cliente ligero.
- Información sobre cualquier incidente ocurrido al habilitar o deshabilitar la administración de Kaspersky Thin Client a través de Kaspersky Security Center Web Console.

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.

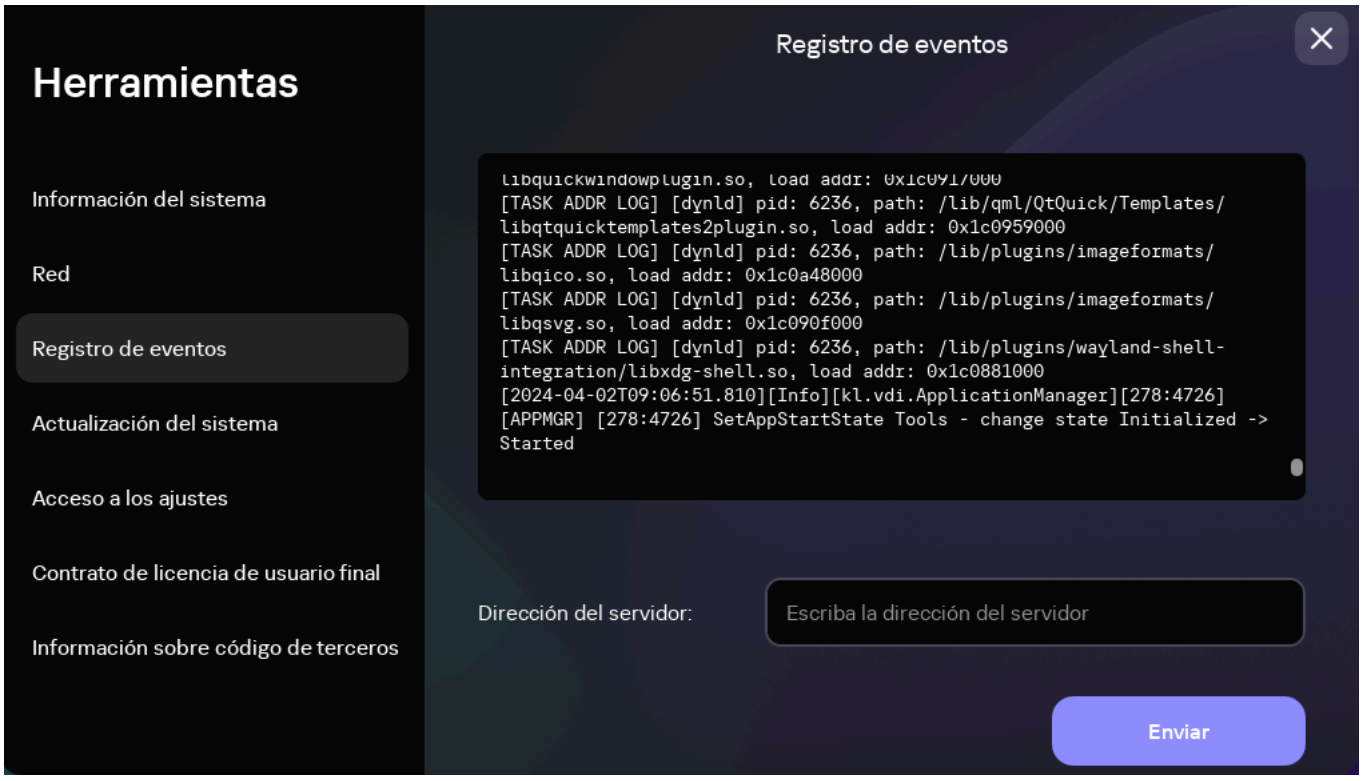
Como primera medida, asegúrese de contar con un servidor de registros instalado en la infraestructura de su organización. Para obtener información detallada sobre cómo instalar un servidor de registros, consulte la guía del administrador de dicho servidor.

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 **Registro de eventos** (vea la siguiente imagen).



Herramientas. Sección **Registro de eventos**

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 Kaspersky Thin Client es miembro de un grupo de administración, se controla de forma centralizada a través de Web Console y la función **Imponer** está habilitada, el campo **Dirección del servidor** tendrá el valor que haya definido el administrador de Kaspersky Security Center y no se podrá modificar.

   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 remitirse a terceros no autorizados. De ocurrir esto, la confidencialidad de los datos contenidos en los registros podría verse afectada.

4. En la ventana que se abre, confirme que desea enviar los registros de eventos y de auditoría.

   Si Kaspersky Thin Client no está en un grupo de administración y los registros de eventos y de auditoría van a reenviarse a un servidor de registros por primera vez, cuando se abra la ventana **Agregar certificado**, controle los parámetros del certificado que se va a agregar y haga clic en **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

Actualización

Procedimiento para reemplazar o agregar archivos nuevos (bases de datos o módulos de Kaspersky Thin Client) obtenidos de los servidores de actualización de Kaspersky.

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 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.

Dispositivos administrados

Dispositivos empresariales conectados a la red e incluidos en un grupo de administración.

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 combinados según las funciones que realizan. Agrupar los dispositivos ayuda a administrarlos en forma conjunta. Un grupo puede incluir otros grupos. Pueden crearse directivas de grupo para cada cliente ligero agregado a un 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.

Servidores de actualización de Kaspersky

Servidores HTTP de Kaspersky desde los cuales la aplicación de Kaspersky obtiene actualizaciones para sus bases de datos y módulos de software.

TLS

Protocolo seguro que utiliza cifrado para transferir datos en redes locales y en Internet.

Web Access

Aplicación para conectarse a escritorios virtuales implementados en una infraestructura de Citrix Workspace y VMware Horizon.

Información sobre el código de terceros

Encontrará información sobre el código de terceros en el archivo LegalNotices_en.txt que forma parte del kit de distribución.

También puede ver información sobre el código de terceros en la interfaz de Kaspersky Thin Client.

Para ver información sobre el código de terceros:

1. 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.

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.

VMware Horizon es una marca registrada y/o una marca comercial de VMware, Inc. en Estados Unidos y otros países.