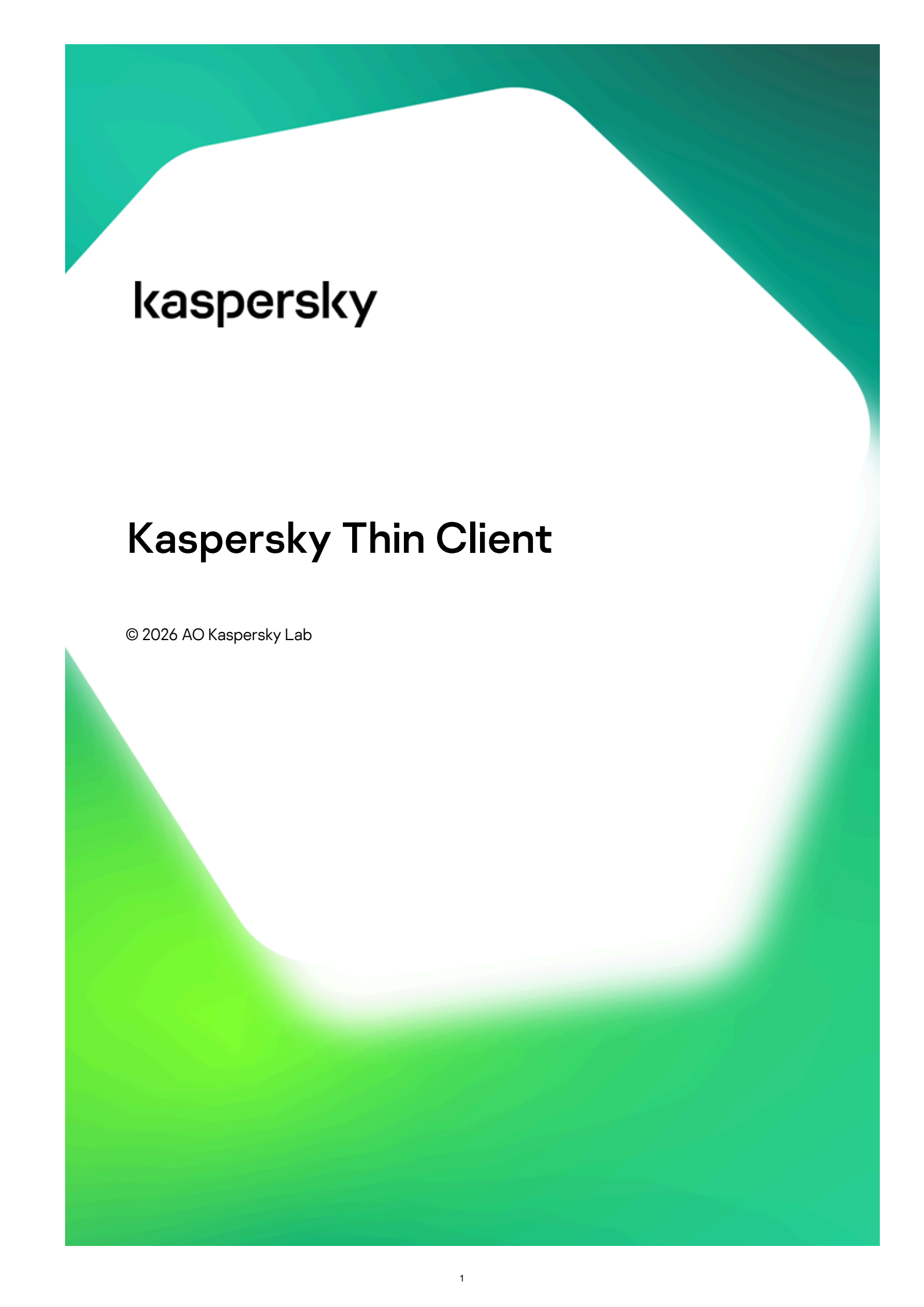


The background of the page is a vibrant green with a white, rounded rectangular shape in the center. The Kaspersky logo is positioned in the upper left of the white shape, and the title 'Kaspersky Thin Client' is centered below it. The copyright notice is located in the lower left of the white shape.

kaspersky

Kaspersky Thin Client

© 2026 AO Kaspersky Lab

Índice

[Ajuda do Kaspersky Thin Client](#)

[Sobre o Kaspersky Thin Client](#)

[Kit de distribuição](#)

[Operação do Kaspersky Thin Client](#)

[Requisitos de hardware e software](#)

[Métodos de conexão remota](#)

[Conexão por meio do aplicativo RDP](#)

[Conexão por meio do aplicativo Basis.WorkPlace](#)

[Conexão por meio do aplicativo Web Access](#)

[Novidades](#)

[Instalação e atualização o Kaspersky Thin Client](#)

[Instalação do Kaspersky Thin Client](#)

[Atualização do Kaspersky Thin Client](#)

[Interface do Kaspersky Thin Client](#)

[Licenciamento do Kaspersky Thin Client](#)

[Provisão de dados](#)

[Primeira ativação do Kaspersky Thin Client](#)

[Reiniciar e desativar o Kaspersky Thin Client](#)

[Uso de certificados no Kaspersky Thin Client](#)

[Configuração do Kaspersky Thin Client](#)

[Cenário: início rápido para administradores](#)

[Cenário: atribuição de certificado para um grupo de thin clients](#)

[Cenário: migração de thin client para um novo servidor do Kaspersky Security Center](#)

[Definição das configurações gerais](#)

[Definição das configurações de rede](#)

[Gerenciamento de dispositivos de reprodução e gravação de áudio](#)

[Definição das configurações de conexão do Kaspersky Thin Client com o Kaspersky Security Center](#)

[Alteração das configurações para conectar o Kaspersky Thin Client ao Kaspersky Security Center](#)

[Configuração da data e a hora](#)

[Configuração da inicialização automática e exibição de aplicativos](#)

[Configuração de monitores e telas](#)

[Definição das configurações de economia de energia](#)

[Definição de configurações de gerenciamento remoto de thin clients na interface do Kaspersky Thin Client](#)

[Alteração do tipo de dispositivos USB não reconhecidos](#)

[Redefinição das configurações do Kaspersky Thin Client](#)

[Definição das configurações de conexão com um ambiente remoto pelo aplicativo RDP](#)

[Definição das configurações de conexão com um ambiente remoto pelo aplicativo Basis.WorkPlace](#)

[Gerenciamento do acesso às configurações do Kaspersky Thin Client](#)

[Gerenciamento do Kaspersky Thin Client instalado em um thin client](#)

[Cenário: funcionamento do Kaspersky Thin Client em um thin client](#)

[Conexão com um ambiente remoto](#)

[Conexão com um ambiente remoto pelo aplicativo RDP](#)

[Conexão com um ambiente remoto pelo aplicativo Basis.WorkPlace](#)

[Conexão com um ambiente remoto por meio do aplicativo Web Access](#)

[Gerenciamento de uma sessão remota](#)

[Uso do painel de conexão](#)

[Bloqueio e desbloqueio de sessão remota](#)

[Encerramento de uma sessão remota](#)

[Gerenciamento de dispositivos de reprodução e gravação de áudio em um painel de conexão](#)

[Gerenciamento de janelas de aplicativos virtuais](#)

[Web Access: redirecionamento de dispositivos USB para um ambiente remoto](#)

[Visualização de informações sobre o Kaspersky Thin Client e um thin client](#)

[Exibição das informações do status da rede](#)

[Exibição das notificações do Kaspersky Thin Client](#)

[Gerenciamento de certificados na interface do Kaspersky Thin Client](#)

[Gerenciamento do Kaspersky Thin Client com o uso de teclas de atalho](#)

[Administração do acesso ao gerenciamento remoto e à tela do ambiente remoto](#)

[Conexão remota com um thin client](#)

[Gerenciamento do Kaspersky Thin Client pelo Kaspersky Security Center Web Console](#)

[Sobre o plug-in da Web do Kaspersky Security Management Suite](#)

[Instalação do plug-in da Web do Kaspersky Security Management Suite](#)

[Atualização do plug-in da Web do Kaspersky Security Management Suite](#)

[Remoção do plug-in da Web do Kaspersky Security Management Suite](#)

[Restrição de acesso às funções do plug-in da Web do Kaspersky Security Management Suite](#)

[Fazendo login e logout do Web Console](#)

[Gerenciamento de políticas e grupos de administração](#)

[Criação de um grupo de administração](#)

[Adição de thin clients ao grupo de administração](#)

[Criação da política](#)

[Edição de uma política](#)

[Bloqueio de configurações em uma política](#)

[Definição das configurações do Kaspersky Thin Client para um dispositivo pelo Web Console](#)

[Alteração de um ID de thin client pelo Web Console: um dispositivo](#)

[Configuração de uma conexão com um ambiente remoto usando o aplicativo RDP pelo Web Console: um dispositivo](#)

[Configuração de uma conexão com um ambiente remoto usando o aplicativo Basis.WorkPlace pelo Web Console: um dispositivo](#)

[Configuração de uma conexão com um ambiente remoto no aplicativo Web Access pelo Web Console: um dispositivo](#)

[Configuração de monitores e telas pelo Web Console: um dispositivo](#)

[Definição das configurações do sistema do Kaspersky Thin Client pelo Web Console: um dispositivo](#)

[Configuração do encaminhamento de logs do Kaspersky Thin Client para um servidor de log: um dispositivo](#)

[Personalização do Kaspersky Thin Client: um dispositivo](#)

[Definição das configurações para conexão remota a um thin client usando o Web Console: um dispositivo](#)

[Configuração da inicialização automática e exibição de aplicativos: um dispositivo](#)

[Definição das configurações do Kaspersky Thin Client para um grupo de administração pelo Web Console](#)

[Definição das principais configurações do Kaspersky Thin Client pelo Web Console: grupo de administração](#)

[Configuração de uma conexão com um ambiente remoto por meio do aplicativo RDP pelo Web Console: grupo de administração](#)

[Configuração de uma conexão com um ambiente remoto usando o aplicativo Basis.WorkPlace pelo Web Console: grupo de administração](#)

[Configuração de uma conexão com um ambiente remoto usando o aplicativo Web Access pelo Web Console: grupo de administração](#)

[Configuração de monitores e telas pelo Web Console: grupo de administração](#)

[Definição das configurações do Kaspersky Thin Client pelo Web Console: grupo de administração](#)

[Configuração do encaminhamento de logs do Kaspersky Thin Client para um servidor de log: grupo de administração](#)

[Personalização do Kaspersky Thin Client: grupo de administração](#)

[Definição das configurações para conexão remota com um thin client usando o Web Console: grupo de administração](#)

[Configuração da inicialização automática e exibição de aplicativos: grupo de administração](#)

[Configuração da sincronização entre o Kaspersky Thin Client e o Kaspersky Security Center](#)

[Confirmação das ações do usuário do Kaspersky Thin Client](#)

[Gerenciamento dos certificados do Kaspersky Thin Client pelo Web Console](#)

[Sobre um certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center](#)

[Reemissão de um certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center com o uso do Web Console](#)

[Criação de um certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center](#)

[Carregamento de um certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center usando o Web Console](#)

[Adição de novos certificados no Web Console](#)

[Remoção dos certificados do Web Console](#)

[Conversão de um certificado do formato PEM para DER](#)

[Atualização de um certificado ao migrar para um novo servidor do Kaspersky Security Center](#)

[Monitoramento de eventos do Kaspersky Thin Client pelo Kaspersky Security Center Web Console](#)

[Configuração do registro das notificações de eventos do Kaspersky Thin Client por meio do Kaspersky Security Center Web Console](#)

[Exibição dos eventos do Kaspersky Thin Client no Web Console](#)

[Solução de problemas](#)

[Reconectar após uma falha de conexão remota](#)

[Problemas de restrição de acesso às funções do plug-in da web do Kaspersky Security Management Suite](#)

[Entrando em contato com o Suporte Técnico](#)

[Informações sobre os logs do Kaspersky Thin Client](#)

[Encaminhamento do log](#)

[Glossário](#)

[Administrador do Kaspersky Security Center](#)

[Ambiente remoto](#)

[Aplicativo virtual](#)

[Broker](#)

[Desktop remoto](#)

[Evento](#)

[Grupo de administração](#)

[Plug-in da Web do Kaspersky Security Management Suite](#)

[Política](#)

[Servidor de Administração](#)

[Servidor de log](#)

[Sessão remota](#)

[Thin client](#)

[TLS](#)

[Informação sobre códigos de terceiros](#)

[Avisos de marcas comerciais](#)

Ajuda do Kaspersky Thin Client

	Novidades Novidades desta versão do Kaspersky Thin Client.		Requisitos de hardware e software Ambientes remotos e dispositivos periféricos compatíveis.
	Instalar e atualizar Instalar o Kaspersky Thin Client em um thin client. Atualizar a versão do Kaspersky Thin Client.		Primeiros passos Iniciando o thin client. Configuração inicial e conexão com o Kaspersky Security Center. Atribuir certificados.
	Conexão com um ambiente remoto Opções disponíveis para se conectar a um ambiente remoto. Conexão com um ambiente remoto. Definição das configurações de conexão.		Controle centralizado por meio do Kaspersky Security Center Web Console Gerenciamento de políticas e grupos de administração. Configuração de thin clients com o Kaspersky Thin Client.
	Recursos avançados Gerenciamento de certificados do Kaspersky Thin Client. Gerenciamento do acesso às configurações do Kaspersky Thin Client.		Monitoramento Visualizar e encaminhar logs de eventos e de auditoria para um servidor de log. Visualizar eventos do Kaspersky Thin Client por meio do Kaspersky Security Center Web Console.
	Gerenciamento remoto Conexão remota a um thin client por meio de seu dispositivo.		Redefinição de configurações e dados Redefinição das configurações e dados do Kaspersky Thin Client.

Sobre o Kaspersky Thin Client

O Kaspersky Thin Client versão 2.3 (aqui também referido como "o sistema") é um sistema operacional de micronúcleo ciberimune para [thin clients](#) baseado no KasperskyOS. O Kaspersky Thin Client foi projetado para se conectar a um ambiente remoto e fornecer um espaço de trabalho nele, incluindo suporte para dispositivos periféricos conectados ao thin client. O Kaspersky Thin Client 2.3 pode ser instalado em thin clients [Dell™ Wyse 3040](#), [Centerm F620](#) e [TONK TN1200](#).

Este documento não fornece uma visão geral dos componentes de hardware do thin client, como controles e conectores, pois essas informações estão disponíveis na documentação do fornecedor do dispositivo onde o Kaspersky Thin Client está instalado.

Funções principais do Kaspersky Thin Client:

- Conecte-se com um ambiente remoto:
 - Conectar-se a desktops remotos e virtuais que executam o sistema operacional [Microsoft® Windows®](#) por meio do Protocolo da Área de Trabalho Remota (RDP) e do Microsoft Remote Desktop Connection Broker.
 - Conectar-se a servidores de terminal que executam o sistema operacional [Microsoft Windows Server®](#) por meio do Protocolo da Área de Trabalho Remota (RDP) e do Microsoft Remote Desktop Connection Broker.
 - Conectar-se a desktops remotos e virtuais que executam o sistema operacional [Linux®](#) por meio do Protocolo da Área de Trabalho Remota (RDP).
 - Conectar-se a aplicativos virtuais, incluindo aqueles disponibilizados na infraestrutura do Microsoft Remote Desktop Services ou que executem o sistema operacional [Microsoft® Windows®](#), por meio do Protocolo da Área de Trabalho Remota (RDP).
 - Conectar-se a desktops virtuais disponibilizados na infraestrutura do [Basis.WorkPlace](#).
 - Conectar-se a desktops virtuais disponibilizados na infraestrutura do [Citrix Workspace™](#).
- Transmitir imagens de tela do ambiente remoto para monitores conectados a um thin client.
- Redirecionar os seguintes [dispositivos conectados ao thin client](#) para um ambiente remoto:
 - teclados e mouses com e sem fio;
 - unidades USB;
 - dispositivos de reprodução e gravação de áudio (fones de ouvido USB);
 - webcams;
 - cartões inteligentes e tokens;
 - dispositivos de impressão e digitalização: impressoras, scanners (inclusive scanners de códigos QR e de códigos de barras).

- Gerenciar, atualizar e monitorar de forma centralizada o Kaspersky Thin Client por meio do [Kaspersky Security Center Web Console](#). O [plug-in da web do Kaspersky Security Management Suite](#) é utilizado para a comunicação entre o Kaspersky Thin Client e o Kaspersky Security Center.

O Kaspersky Thin Client 2.3 é compatível com o Kaspersky Security Center Linux versão 15.3 e o Kaspersky Security Center Web Console versão 15.3.

O Kaspersky Thin Client 2.3 é compatível com os seguintes idiomas de interface: russo, inglês (EUA), espanhol (México) e português (Brasil).

Kit de distribuição

O Kaspersky Thin Client 2.3 é oferecido em um dos seguintes formatos:

- a imagem do Kaspersky Thin Client sem uma plataforma de hardware (thin client)
- plataforma de hardware fornecida pelo parceiro com o Kaspersky Thin Client pré-instalado

O kit de distribuição do Kaspersky Thin Client sem uma plataforma de hardware inclui os seguintes arquivos:

- `Kaspersky_Thin_Client_2.3.0.<versão de compilação técnica>_Wyse3040.tar.gz`: arquivo que contém a imagem de instalação do Kaspersky Thin Client para a plataforma Dell Wyse 3040.
- `Kaspersky_Thin_Client_2.3.0.<versão de compilação técnica>_TN1200.tar.gz`: arquivo que contém a imagem de instalação do Kaspersky Thin Client para as plataformas TONK TN1200 e Centerm F620.
- `hw_install.sh`: script para instalação no thin client.
- Scripts para atualização das versões comerciais 2.0 e 2.0.1 para a versão 2.3:
 - `hw_update.sh`
 - `save_files.sh`
 - `restore_files.sh`
- `KTC_LegalNotices_en.txt`: o arquivo de texto que contém as informações sobre códigos de terceiros.
- Os arquivos de texto que descrevem novos recursos e limitações conhecidas:
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<versão de compilação técnica>_EN.txt`
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<versão de compilação técnica>_ES.txt`
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<versão de compilação técnica>_PT_BR.txt`
 - `ReleaseNotes_Kaspersky_Thin_Client_2.3.0.<versão de compilação técnica>_RU.txt`
- Os arquivos do Contrato de Licença de Usuário Final do Kaspersky Thin Client:
 - `eula_en_ktc_00008.txt`
 - `eula_es_ktc_00008.txt`

- eula_pt_ktc_00008.txt
- eula_ru_ktc_00008.txt

O kit de distribuição do Kaspersky Security Management Suite versão 2.3 abrange os componentes listados abaixo.

Ao descompactar o arquivo comprimido usando as ferramentas de automação, como um script, é necessário ler e aceitar os termos e condições do Contrato de Licença de Usuário Final antes de usar o Kaspersky Security Management Suite.

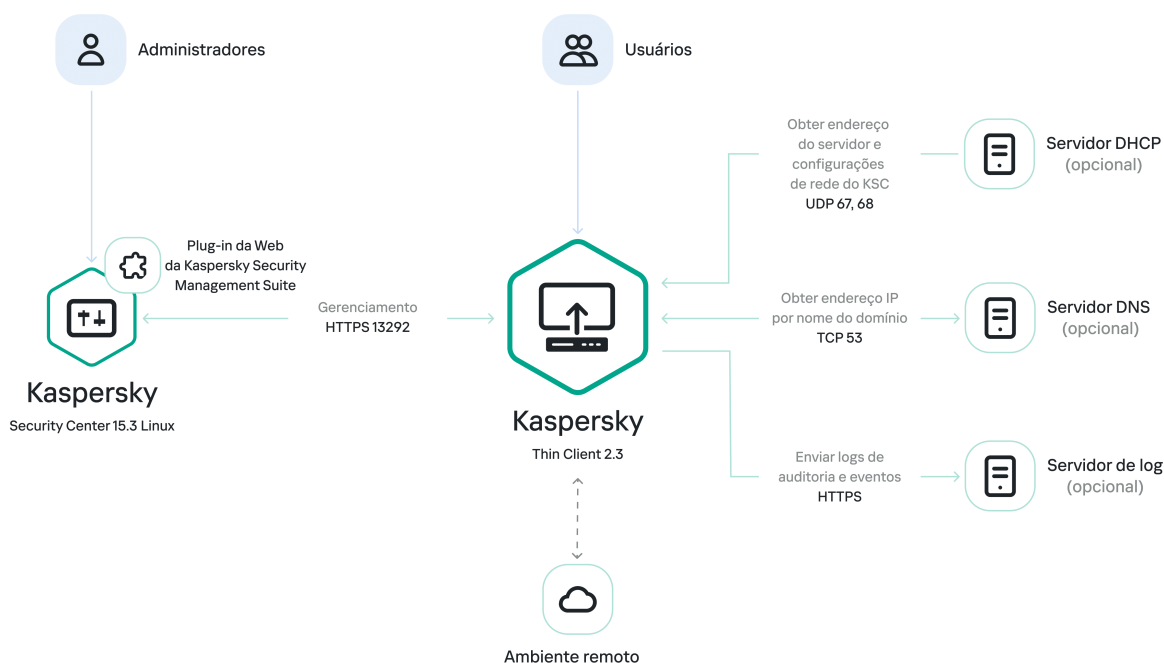
- Arquivos do Linux que contêm as imagens de instalação e os arquivos de assinatura do plug-in da web para o Kaspersky Security Center:
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versão de compilação técnica>_en.sh
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versão de compilação técnica>_es.sh
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versão de compilação técnica>_pt_br.sh
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versão de compilação técnica>_ru.sh
- Os arquivos do Microsoft Windows que contêm as imagens de instalação e os arquivos de assinatura do plug-in da web para o Kaspersky Security Center:
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versão de compilação técnica>_ru.exe
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versão de compilação técnica>_en.exe
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versão de compilação técnica>_es.exe
 - Web_Plugin_Kaspersky_Security_Management_Suite_2.3.0.<versão de compilação técnica>_pt_br.exe
- KSMS_2_3_0_0.conf: arquivo de configuração RBAC.
- KSMS_LegalNotices_en.txt: o arquivo de texto que contém as informações sobre códigos de terceiros para o Kaspersky Security Management Suite.
- Os arquivos do Contrato de Licença de Usuário Final do Kaspersky Security Management Suite:
 - eula_en_ksms_2.3.rtf
 - eula_es_ksms_2.3.rtf

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

Operação do Kaspersky Thin Client

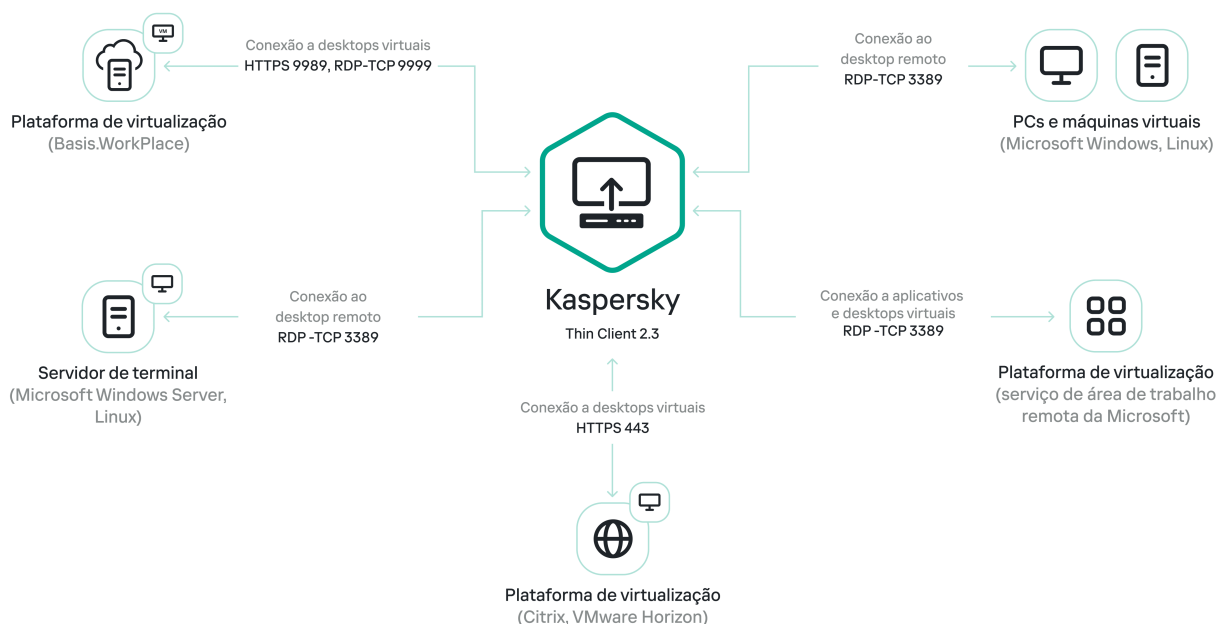
O cenário operacional padrão do Kaspersky Thin Client (consulte a figura abaixo) envolve os seguintes aspectos:

- Depois que o sistema Kaspersky Thin Client for instalado no thin client, ele receberá as configurações de rede de um servidor DHCP. O administrador também pode definir essas configurações de forma manual.
- O administrador deverá conectar e configurar a interação entre o Kaspersky Thin Client e o Kaspersky Security Center, e também instalar o [plug-in da web](#) do Kaspersky Security Management Suite.
- O Kaspersky Thin Client obtém certificados confiáveis, configurações de conexão de ambiente remoto, de data e hora e outras configurações básicas usando uma [política](#) criada por meio do Kaspersky Security Center Web Console.
- O usuário se conectará ao [ambiente remoto](#).
- Em caso de problemas, o usuário encaminhará [logs de auditoria e de eventos](#) por meio da interface do Kaspersky Thin Client para um [servidor de log](#) implementado na infraestrutura da empresa dele.
- O administrador [atualiza o Kaspersky Thin Client](#).



Cenário operacional padrão do Kaspersky Thin Client

A imagem abaixo mostra um diagrama da comunicação do Kaspersky Thin Client com plataformas de virtualização e ambientes remotos.



Comunicação entre o Kaspersky Thin Client e plataformas de virtualização e ambientes remotos

Requisitos de hardware e software

Esta seção descreve os requisitos de hardware e software do Kaspersky Thin Client 2.3.

Este documento não fornece uma visão geral dos componentes de hardware do thin client, como controles e conectores, pois essas informações estão disponíveis na documentação do fornecedor do dispositivo onde o Kaspersky Thin Client está instalado.

Requisitos do monitor

O Kaspersky Thin Client é compatível com a conexão de dois monitores.

Dependendo das configurações de orientação da tela, o Kaspersky Thin Client é compatível com as seguintes resoluções de monitor:

- Se a orientação da tela estiver definida como paisagem ou paisagem invertida:
 - 1024x768 (XGA)
 - 1280x720 (HD)
 - 1280x1024 (SXGA)
 - 1280x768 (WXGA)

- 1440x900 (WXGA+)
- 1400x1050 (SXGA+)
- 1920x1080 (Full HD)
- Se a orientação da tela estiver definida como retrato ou retrato invertido:
 - 1280x1024 (SXGA)
 - 1400x1050 (SXGA+)
 - 1920x1080 (Full HD)

O Kaspersky Thin Client é compatível com as seguintes interfaces de conexão:

- HDMI
- DisplayPort

O Kaspersky Thin Client é compatível apenas com monitores True Color.

Requisitos para dispositivos periféricos conectados ao Kaspersky Thin Client

O Kaspersky Thin Client é compatível com os seguintes dispositivos periféricos:

- Teclados e mouses USB sem recursos multimídia e teclados e mouses sem fio (rádio).
- Unidades USB.
- Cartões inteligentes e tokens USB.
- Dispositivos de impressão e digitalização conectados por USB: impressoras, scanners (inclusive scanners de códigos QR e de códigos de barras).

Um driver para o dispositivo conectado ao thin client deve ser instalado no ambiente remoto.

- Dispositivos de gravação e reprodução de áudio com fio conectados a um miniconector e via porta USB, e fones de ouvido USB sem fio (rádio).
- Webcams conectadas via porta USB.

Requisitos para sistemas de virtualização e acesso remoto

O Kaspersky Thin Client é compatível com os seguintes sistemas de virtualização e acesso remoto:

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

Requisitos de rede

A velocidade de transmissão da rede deve ser de pelo menos 50 Mbit/s.

Requisitos do Kaspersky Security Center e do Kaspersky Security Center Web Console

O sistema Kaspersky Thin Client é compatível com a versão 15.3 do Kaspersky Security Center para Linux. Os requisitos de sistema e de software para o servidor onde o Kaspersky Security Center será implementado são exibidos no [guia da ajuda on-line do Kaspersky Security Center](#).

Requisitos do servidor de log

O [servidor de log](#) deve atender aos seguintes requisitos:

- O Kaspersky Thin Client se conecta ao servidor de log por HTTPS (a porta 443 é usada por padrão).
- O Kaspersky Thin Client se conecta ao servidor de log baseado apenas no certificado de segurança.
- O Kaspersky Thin Client envia [logs de auditoria e de eventos](#) para o servidor de log por meio do método PUT.

Para obter instruções sobre como instalar e configurar o servidor de log, consulte a [Base de conhecimento](#).

Métodos de conexão remota

Esta seção contém informações sobre tecnologias de conexão remota e [ambientes remotos](#) compatíveis com o Kaspersky Thin Client, bem como as maneiras de se conectar a esses ambientes com o uso dos aplicativos do Kaspersky Thin Client.

O Kaspersky Thin Client usa os seguintes aplicativos:

- **RDP** para conexão com desktops remotos ou aplicativos virtuais via protocolo RDP.
- **Basis.WorkPlace** para conexão com desktops virtuais implementados na infraestrutura Basis.WorkPlace.
- **Web Access**: para conectar com um ambiente remoto implementado em uma infraestrutura Citrix Workspace.

Esta seção fornece informações sobre quais dispositivos conectados com o Kaspersky Thin Client podem ser redirecionados para um ambiente remoto.

Conexão por meio do aplicativo RDP

No Kaspersky Thin Client, é possível se conectar via RDP a um ambiente remoto, como o Microsoft Remote Desktop Services (MS RDS). A tabela abaixo descreve os métodos de conexão disponíveis e os periféricos para os sistemas operacionais Windows e Linux.

A partir da versão 2.3.4, o Kaspersky Thin Client permite a conexão imediata de tokens, unidades e impressoras USB, sem interromper a sessão remota ativa.

Para redirecionar os periféricos para um desktop remoto do Linux, instale o Kaspersky USB Redirector para o servidor xRDP no sistema operacional visitante. O Kaspersky USB Redirector não está incluído no kit de distribuição. Você pode solicitar a extensão da Kaspersky.

As instruções para conectar a um ambiente remoto são fornecidas em um [artigo separado](#).

RDP: sistemas operacionais, métodos de conexão e periféricos compatíveis

	Windows Server 2016/2019/2022 no MS RDS	Windows 10/11	Windows Server 2016/2019/2022	ALT Linux 11 RED OS 8	Astra Linux SE 1.8.1
Conexão com um aplicativo virtual	✓	✓	✓	—	—
Conexão com um desktop remoto					
Conexão direta	—	✓	✓	✓	✓
Conexão usando VDI	✓	—	—	—	—
Conexão do terminal	✓	—	✓	✓	✓
Dispositivos periféricos					
Tokens USB	✓	✓	✓	✓ Observação	—
Cartões inteligentes (USB)	✓	✓	✓	✓ Observação	—

Unidades USB	✓	✓	✓	✓ Observação ?	—
Impressoras (USB)	✓	✓	✓ Observação ?	✓ Observação ?	—
Scanners (USB)	✓	✓	✓ Observação ?	✓ Observação ?	—
Leitores de código QR e código de barras (USB)	✓	✓	✓	✓	✓
Microfones (minitomada, USB) Observação ?	✓	✓	✓ Observação ?	✓ Observação ?	✓ Observação ?
Dispositivos de reprodução de áudio (minitomada, USB) Observação ?	✓	✓	✓ Observação ?	✓ Observação ?	✓ Observação ?
Câmera da Web (vídeo, USB)	✓	✓	✓	—	—

Conexão por meio do aplicativo Basis.WorkPlace

O Kaspersky Thin Client pode se conectar a um ambiente remoto do Basis.WorkPlace. A tabela abaixo descreve os métodos de conexão disponíveis e os periféricos para os sistemas operacionais Windows e Linux.

Para redirecionar os periféricos para um desktop remoto do Linux, instale o Kaspersky USB Redirector para o servidor xRDP no sistema operacional visitante. O Kaspersky USB Redirector não está incluído no kit de distribuição. Você pode solicitar a extensão da Kaspersky.

As instruções para conectar a um ambiente remoto são fornecidas em um [artigo separado](#).

Basis.WorkPlace: sistemas operacionais compatíveis, métodos de conexão e periféricos

	Windows 10/11	Windows Server 2016/2019/2022	RED OS 8 ALT Linux 11 Astra Linux SE 1.8.1
Conexão com um desktop remoto			
Conexão direta ?	—	—	—
Conexão usando VDI ?	✓	✓	✓
Conexão do terminal ?	—	✓	—
Dispositivos periféricos			
Tokens USB	✓	✓	—
Cartões inteligentes (USB)	✓	✓	—
Unidades USB	✓	✓	—
Impressoras (USB)	✓	✓ Observação ?	—
Scanners (USB)	✓	✓	—
Leitores de código QR e código de barras (USB)	✓	✓	—
Microfones (minitomada, USB) Observação ?	✓	✓	✓

Dispositivos de reprodução de áudio (minitomada, USB) Observação ?	✓	✓	✓
Câmera da Web (vídeo, USB)	—	—	—

Conexão por meio do aplicativo Web Access

É possível usar o aplicativo Web Access para se conectar a um ambiente remoto implementado nas infraestruturas do Citrix Workspace. O Web Access é compatível com HTML5 e fornece uma conexão HTTPS segura ao conectar. A tabela abaixo descreve os métodos de conexão específicos e os dispositivos periféricos que estão disponíveis para os sistemas operacionais Windows.

As instruções de conexão são fornecidas em um [artigo separado](#).

Web Access: sistemas operacionais compatíveis, métodos de conexão e periféricos

	Microsoft Windows 10/11	Microsoft Windows Server 2016/2019/2022
Conexão com um desktop remoto		
Conexão direta ?	—	—
Conexão usando VDI ?	✓	✓
Conexão do terminal ?	—	✓
Dispositivos periféricos (Citrix Workspace)		
Tokens USB	—	—
Cartões inteligentes (USB)	—	—
Unidades USB (FAT16 e FAT32, até 128 GB)	✓	✓
Impressoras (USB)	✓	✓
Scanners (USB)	✓	✓
Leitores de código QR e código de barras (USB)	✓	✓
Microfones (minitomada, USB) Observação ?	✓	✓
Dispositivos de reprodução de áudio (minitomada, USB) Observação ?	✓	✓
Câmera da Web (vídeo, USB)	✓	✓

A versão atual do Kaspersky Thin Client não é compatível com a conexão para desktops remotos que executam Linux ou usam o aplicativo Web Access para se conectar com a aplicativos virtuais.

Não há suporte para o redirecionamento de mais de dois dispositivos USB simultaneamente ao se conectar com um ambiente remoto implementado na infraestrutura do Citrix Workspace.

Novidades

O Kaspersky Thin Client versão 2.3 tem os seguintes novos recursos e melhorias:

- Redirecionamento dos seguintes dispositivos para um ambiente virtual Citrix usando o aplicativo Web Access:
 - unidades USB (via mapeamento de unidade cliente);
 - fones de ouvido USB;
 - webcams;
 - dispositivos de impressão e digitalização: impressoras, scanners (inclusive leitores de códigos de barras e códigos QR).
- Redirecionamento dos seguintes dispositivos para um ambiente remoto via RDP:
 - fones de ouvido USB;
 - webcams;
 - dispositivos de impressão e digitalização: impressoras, scanners (inclusive leitores de códigos de barras e códigos QR).
- Adicionada a capacidade de selecionar um dispositivo de reprodução e gravação de áudio no painel de conexão durante uma sessão remota.
- Adicionada a capacidade de definir as seguintes configurações para se conectar com um desktop remoto de thin client via RDP:
 - conexão do administrador ao desktop remoto de thin client (automática, confirmação do usuário ou negada);
 - exibe uma sessão remota do usuário ao administrador: automaticamente, com confirmação do usuário ou não permitida.
- Suporte para conexão remota com um thin client pelo protocolo RDP com autorização por nome do dispositivo e senha.
- Suporte para bloquear a tela do thin client por meio de uma sessão remota ativa.
- Adicionado suporte para o thin client Dell Wyse 3040.
- Suporte para firmware UEFI que aumenta a velocidade de inicialização do thin client, além de ser compatível com grandes quantidades de memória.
- Adicionada a capacidade de exibir no desktop do thin client apenas os aplicativos selecionados pelo usuário nas configurações (RDP, Basis.WorkPlace ou Web Access).
- Adicionada a capacidade de iniciar automaticamente um dos aplicativos (RDP, Basis.WorkPlace ou Web Access) conforme selecionado pelo usuário na inicialização do thin client.
- Adicionada a capacidade de se conectar automaticamente a um ambiente remoto após iniciação do RDP.

- Adicionado um assistente de seleção de idioma para a primeira inicialização do Kaspersky Thin Client.
- Adicionada a capacidade de definir um plano de fundo personalizado no desktop do Kaspersky Thin Client por meio do Kaspersky Security Center Web Console.
- Adicionada a capacidade de definir uma tela inicial personalizada na tela de bloqueio do Kaspersky Thin Client por meio do Kaspersky Security Center Web Console.
- Adicionada a capacidade de configurar monitores centralmente por meio do Kaspersky Security Center Web Console, inclusive as seguintes configurações:
 - resolução e orientação da tela
 - modo de exibição (desktop duplicado ou estendido) da tela não principal
- Adicionada a capacidade de definir manualmente o tipo do dispositivo conectado incapaz de ser reconhecido pelo sistema.
- Suporte para redirecionamento de um fone de ouvido USB sem fio, teclado ou mouse (via rádio) para um ambiente remoto.
- Adicionado suporte para os seguintes idiomas de entrada: alemão (de-DE), francês suíço (fr-CH) e alemão suíço (de-CH).
- Adicionada a capacidade de fixar ou ocultar completamente o painel de conexão em um ambiente remoto.
- Adicionada a capacidade de [redirecionar](#) os seguintes tokens via RDP para um desktop remoto RED OS 8.0 e, em seguida, para um desktop remoto do Windows 10, desde que uma sessão de desktop remoto esteja sendo iniciada entre esses desktops:
 - Rutoken Lite
 - JaCarta-2 PKI/GOST
- Suporte para a nova versão do [Kaspersky Security Center Web Console](#), 15.3.
- Design e texto aprimorados da interface do usuário do Kaspersky Thin Client e do [Kaspersky Security Management Suite](#).

Instalação e atualização o Kaspersky Thin Client

O procedimento de instalação do Kaspersky Thin Client depende do [formato de entrega](#):

- Um parceiro fornece uma plataforma de hardware com o Kaspersky Thin Client pré-instalado. Neste caso, a instalação do Kaspersky Thin Client na plataforma de hardware é feita pela TONK.
- O Kaspersky Thin Client é oferecido sem uma plataforma de hardware (thin client). Nesse caso, a plataforma de software é instalada de acordo com as instruções fornecidas nesta seção.

Instalação do Kaspersky Thin Client

Antes de instalar o Kaspersky Thin Client, faça o seguinte:

1. Prepare uma unidade USB inicializável que contenha o sistema operacional Linux Ubuntu (versão recomendada: Ubuntu 20.04).
2. Copie os arquivos de instalação do Kaspersky Thin Client recebidos no [kit de distribuição](#) em uma partição separada na unidade USB inicializável ou em uma unidade USB separada:
 - Kaspersky_Thin_Client_<número da versão>_Wyse3040.tar.gz ou Kaspersky_Thin_Client_<número da versão>_TN1200.tar.gz: imagem de instalação;
 - hw_install.sh: script de instalação do Kaspersky Thin Client.

Para garantir a segurança antes da instalação do Kaspersky Thin Client, recomendamos atualizar a BIOS no thin client para a versão mais recente, definir uma senha para as alterações de configuração da BIOS e configurar a opção para inicializar somente a partir de um dispositivo SSD local. Essas medidas recomendadas ajudarão a evitar possíveis riscos de segurança, como substituição do sistema operacional, substituição ou exclusão de certificados de conexão do servidor remoto e acesso não autorizado às configurações do sistema operacional.

O Kaspersky Thin Client é compatível com a tecnologia Secure Boot que permite à UEFI verificar a autenticidade dos componentes carregados. Caso queira configurar a Inicialização segura, será possível obter as chaves necessárias com os especialistas da Kaspersky, e, além disso, usar as instruções da [Base de conhecimento](#).

Para instalar o Kaspersky Thin Client em um thin client:

1. Insira a unidade USB inicializável preparada na [porta correspondente](#) do thin client.
2. [Ative o thin client](#) e inicie a imagem do Ubuntu na unidade USB inicializável sem instalar o sistema no disco rígido do thin client.
3. Após o carregamento do sistema operacional, acesse o diretório que contém os arquivos de instalação do Kaspersky Thin Client.

4. Execute o seguinte comando:

```
sudo bash ./hw_install.sh -u Kaspersky_Thin_Client_<número da versão>_<nome da
plataforma>.tar.gz
```

onde:

- `./hw_install.sh`: caminho para o script de instalação;
- `Kaspersky_Thin_Client_<número da versão>_<nome da plataforma>.tar.gz`: imagem de instalação.

A mensagem *Installed OK! Remove USB drive and reboot* é exibida após a instalação bem-sucedida.

5. Desative o thin client e remova a unidade USB inicializável.

O sistema Kaspersky Thin Client será carregado na próxima vez que você ativar o thin client.

É possível verificar o número da versão atual do SO na [interface do Kaspersky Thin Client](#).

Atualização do Kaspersky Thin Client

É possível atualizar o Kaspersky Thin Client da versão 2.0 ou 2.0.1 para a versão 2.3.

Antes de atualizar o Kaspersky Thin Client, faça o seguinte:

1. Prepare uma unidade USB inicializável contendo a distribuição Linux. Recomendamos usar o Linux Ubuntu (versão recomendada: Ubuntu 20.04).
2. Verifique e confirme se o utilitário OpenSSL está instalado no sistema. Caso não esteja instalado, instale-o executando o seguinte comando:

```
sudo apt install openssl
```

3. Copie os seguintes arquivos do kit de distribuição do Kaspersky Thin Client 2.3 em um diretório na unidade USB:

- Arquivo comprimido que contém a imagem de instalação `Kaspersky_Thin_Client_<número da versão>_TN1200.tar.gz`.
- Scripts de instalação e atualização:
 - `hw_install.sh`
 - `hw_update.sh`
 - `save_files.sh`
 - `restore_files.sh`

Para atualizar o Kaspersky Thin Client em um thin client:

1. Insira a unidade USB inicializável preparada na porta correspondente do thin client.
2. [Ative o thin client](#) e execute a imagem do Ubuntu na unidade USB inicializável sem instalar o sistema no disco rígido do thin client. Para fazê-lo, selecione a opção *Try without installation*.

3. No sistema operacional em execução, acesse o diretório que contém os scripts e a imagem de instalação do Kaspersky Thin Client 2.3.

4. Execute o script de atualização com o seguinte comando:

```
sudo bash ./hw_update.sh -u <caminho para o arquivo comprimido que contém a imagem de instalação do Kaspersky Thin Client>
```

Caso o script de atualização seja concluído com êxito, a mensagem *Updated OK!* será exibida.

Caso ocorra um erro durante a execução do script, [entre em contato com os contatos do Suporte Técnico.](#)

5. Desative o thin client e remova a unidade USB inicializável.

A atualização foi concluída. Na próxima vez que o dispositivo for ligado, será possível usar o Kaspersky Thin Client 2.3.

Interface do Kaspersky Thin Client

A interface do Kaspersky Thin Client contém os seguintes elementos:

- desktop com aplicativos
- painel de controle na parte superior da janela
- painel de conexão exibido durante uma sessão remota

Desktop

A parte central do desktop do Kaspersky Thin Client exibe os aplicativos que podem ser usados para conexão com um [ambiente remoto](#).

- **RDP:** conexão com os desktops remotos ou aplicativos virtuais via protocolo RDP.
- **Basis.WorkPlace:** conecta a desktops virtuais implementados na infraestrutura Basis.WorkPlace.
- **Web Access:** conexão com um ambiente remoto implementado em uma infraestrutura Citrix Workspace.

Painel de controle

O painel de controle do Kaspersky Thin Client contém os seguintes elementos:

-  é um botão do menu de desligamento.
Nele, é possível [encerrar](#) ou [reiniciar](#) o Kaspersky Thin Client.
-  é um botão para mudar para as seções **Configurações** e **Ferramentas**:
Na seção **Configurações**, é possível [configurar o Kaspersky Thin Client](#).
Na seção **Ferramentas**, é possível fazer o seguinte:
 - [exibir as informações sobre o Kaspersky Thin Client](#)
 - [exibir as informações sobre o status da rede](#)
 - [exibir e encaminhar os logs de eventos do Kaspersky Thin Client](#)
 - exibir as informações sobre as atualizações do Kaspersky Thin Client
 - [visualizar o Contrato de Licença de Usuário Final atual](#)
 - [exibir as informações sobre códigos de terceiros](#)
 - [gerenciar o acesso às configurações do Kaspersky Thin Client](#)
-  é um botão para abrir a janela que contém [informações sobre o thin client e os contatos do Suporte Técnico](#).
- [Status da conexão de rede do Kaspersky Thin Client](#)

-  é um botão para abrir o [painel de notificações](#).
- Botão para [alternar o idioma de entrada do teclado](#).
- [Data e hora do sistema](#).
-  é um botão para abrir o menu de [gerenciamento remoto do Kaspersky Thin Client](#).

Painel de conexão

[Painel de conexão](#) exibido durante uma [sessão remota](#) .

Os seguintes itens são exibidos no painel de conexão enquanto houver conexão com um desktop remoto:

-  é um botão para [encerrar uma sessão remota](#).
- Nome da conexão.
- Status da conexão.
-  é um botão para abrir a janela que contém [informações sobre o thin client e os contatos do Suporte Técnico](#).
-  é um botão para [bloquear uma sessão remota](#).
-  é um botão para abrir o [painel de notificações](#).
- Ícone de status da rede.
-  é um botão que abre a janela em que é possível [gerenciar dispositivos de gravação e reprodução de áudio](#).
O botão é exibido caso haja dois ou mais dispositivos desse tipo conectados ao thin client.
-  é um botão que abre a janela em que é possível [gerenciar o redirecionamento de dispositivos USB](#).
O botão é exibido [ao conectar a um ambiente remoto implantado em uma infraestrutura Citrix Workspace](#).

O painel de conexão também exibe os seguintes elementos quando houver conexão com um aplicativo virtual:

- ícone do aplicativo
- data atual definida no Kaspersky Thin Client
- hora atual definida no Kaspersky Thin Client
- idioma da interface do Kaspersky Thin Client

Licenciamento do Kaspersky Thin Client

Os termos de uso do Kaspersky Thin Client são definidos no Contrato de Licença de Usuário Final ou em um documento semelhante que regula o uso do sistema.

O *Contrato de Licença de Usuário Final* é um contrato que vincula o usuário e a AO Kaspersky Lab, e define os termos sob os quais o Kaspersky Thin Client pode ser usado.

Leia com atenção os termos e as condições do Contrato de Licença de Usuário Final antes de começar a trabalhar com o Kaspersky Thin Client.

Você aceita os termos e as condições do Contrato de Licença de Usuário Final, confirmando que concorda com o texto do Contrato de Licença de Usuário Final quando o sistema for iniciado pela primeira vez. Caso você não aceite os termos e as condições do Contrato de Licença de Usuário Final, você deve cancelar a inicialização do Kaspersky Thin Client e parar de usar o aplicativo. Quando o [Kaspersky Thin Client é atualizado](#), quaisquer alterações aos termos e condições do Contrato de Licença de Usuário Final da nova versão do Kaspersky Thin Client são aceitas pelo administrador do Kaspersky Security Center.

Caso necessário, é possível visualizar o texto do Contrato de Licença de Usuário Final na interface do Kaspersky Thin Client.

Para visualizar o texto do Contrato de Licença de Usuário Final,

no painel de controle do Kaspersky Thin Client, clique em  e selecione **Ferramentas** → **Contrato de Licença de Usuário Final** no menu aberto.

Isso abre uma janela que mostra o texto do Contrato de Licença de Usuário Final para a versão atual do Kaspersky Thin Client.

Provisão de dados

O Kaspersky Thin Client não envia nenhum dado para a Kaspersky. Os dados são processados nos [thin clients](#) com o Kaspersky Thin Client instalado e nos servidores de infraestrutura local que interagem com o Kaspersky Thin Client.

O Kaspersky Thin Client salva as seguintes informações no thin client:

- [Log de eventos](#) contendo os dados técnicos sobre a operação do sistema e as informações sobre os eventos do Kaspersky Thin Client enviados para o Servidor de Administração do Kaspersky Security Center.
- O [Log de auditoria](#) contem os seguintes eventos e seus detalhes:
 - adição, substituição e alternância de certificados para conexão com o Kaspersky Security Center na interface do Kaspersky Thin Client;
 - redefinição de fábrica do Kaspersky Thin Client;
 - aceitação de uma conexão remota ao thin client;
 - criação de um novo arquivo de log de auditoria em caso de rotação de log;
 - salvamento e exclusão da senha do usuário para a conexão automática a um ambiente remoto;
 - ativação (manual e automaticamente) e desativação do gerenciamento do Kaspersky Thin Client por meio do Kaspersky Security Center.
- Configurações do sistema:
 - Data e hora de instalação do Kaspersky Thin Client no thin client.
 - Nome do thin client.
 - Versão atualmente instalada do Kaspersky Thin Client.
 - Idioma da interface do Kaspersky Thin Client.
 - Lista de idiomas disponíveis ao alternar o idioma de entrada do teclado.
 - Localização (coordenadas) do painel de conexão.
 - Os certificados de tempo anteriores eram usados para autenticação ao conectar com brokers, desktops remotos ou aplicativos virtuais via RDP, desktops remotos do Basis.WorkPlace, ambientes remotos no Web Access ou um servidor de log.
 - Dispositivo de gravação e reprodução de som selecionado como principal.
 - Lista de aplicativos exibidos no desktop do Kaspersky Thin Client.
 - Aplicativo selecionado pelo usuário para inicialização automática.
 - Lista de dispositivos USB não reconhecidos com o tipo definido manualmente.

- Arquivos de tela de bloqueio e de plano de fundo da área de trabalho instalados no thin client com seus respectivos metadados.
- Configurações dos monitores conectados:
 - monitores principal e secundário;
 - ID dos monitores principal e secundário;
 - resolução dos monitores principal e secundário;
 - orientação dos monitores principal e secundário;
 - modo de exibição para um monitor secundário.
- Configurações de interação do Kaspersky Security Center:
 - endereço (nome ou endereço IP e porta) do Servidor de Administração do Kaspersky Security Center;
 - método de conexão do Kaspersky Security Center (manualmente ou via DHCP);
 - conjunto de identificadores do Kaspersky Thin Client para conexão com o Kaspersky Security Center;
 - período de sincronização entre o Kaspersky Thin Client e o Kaspersky Security Center em minutos;
 - número de certificados recebidos do Kaspersky Security Center para autenticar conexões do Kaspersky Thin Client com brokers, desktops remotos ou aplicativos virtuais via RDP, desktops remotos do Basis.WorkPlace, ambientes remotos no Web Access ou um servidor de log;
 - impressão digital do certificado atual para autenticar a conexão do Kaspersky Thin Client com o Kaspersky Security Center;
 - padrão de nomenclatura do thin client definido pelo administrador do Kaspersky Security Center (nome do thin client, ID e detalhes adicionais);
 - conjunto de segredos para confirmar as ações do usuário na interface do Kaspersky Thin Client: redefinir dados e configurações, desconectar o thin client do Kaspersky Security Center e substituir o certificado para conectar o thin client ao Kaspersky Security Center;
 - detalhes de contato do Suporte Técnico;
 - arquivos de certificado para autenticar a conexão do Kaspersky Thin Client com o Kaspersky Security Center.
- Configurações de conexão do Web Access:
 - endereço da Web do servidor;
 - arquivos de certificado para autenticação de conexão;
 - dados necessários para trabalhar no ambiente remoto, como arquivos de cookie.

- Configurações de conexão do Basis.WorkPlace:
 - endereço (nome ou endereço IP e porta) do gerenciador de conexões Basis.WorkPlace;
 - nome de usuário para conexão com o gerenciador de conexões Basis.WorkPlace;
 - arquivos de certificado para autenticar o broker ao se conectar com um desktop remoto gerenciado pelo Basis.WorkPlace;
 - ID do Kaspersky Thin Client;
 - número de tentativas de reconexão;
 - perfil de conexão entre o Kaspersky Thin Client e o broker Basis.WorkPlace;
 - configurações para redirecionar periféricos para o desktop remoto: ativar/desativar o redirecionamento de unidades USB e cartões inteligentes;
 - se o uso de dois monitores está ativado ou desativado;
 - lista de endereços (nome ou endereço IP e porta) de gerenciadores de conexões de uma instalação distribuída geograficamente gerenciada pelo Basis.WorkPlace.
- Configurações de conexão do servidor RDP:
 - Endereço (nome ou endereço IP e porta) do servidor Remote Desktop Connection Broker.
 - Domínio e nome de usuário para conexão com o servidor do Remote Desktop Connection Broker.
 - ID da coleta do Remote Desktop Connection Broker.
 - Apelido do aplicativo.
 - Arquivos de certificado para autenticar o servidor Remote Desktop Connection Broker ao se conectar com um desktop remoto ou aplicativo virtual via RDP.
 - Configurações para redirecionar os dispositivos periféricos para o desktop remoto:
 - se o redirecionamento de unidades USB está ativado ou desativado;
 - se o redirecionamento de cartões inteligentes está ativado ou desativado;
 - se o redirecionamento de impressoras está ativado ou desativado;
 - se o redirecionamento dos dispositivos de reprodução de áudio está ativado ou desativado;
 - se o redirecionamento dos dispositivos de registro de áudio está ativado ou desativado;
 - se o redirecionamento do fluxo de vídeo da webcam é permitido;
 - se o redirecionamento de scanners está ativado ou desativado.
 - Caso o uso de dois monitores esteja ativado ou desativado.

- Caso a conexão automática com o desktop remoto ou aplicativo virtual após uma desconexão inesperada esteja ativada ou desativada.
- Configurações de qualidade da imagem:
 - se a suavização de fonte está ativada ou desativada;
 - se a animação do menu está ativada ou desativada;
 - se o plano de fundo da área de trabalho é exibido;
 - se o conteúdo da janela é mostrado ao arrastar;
 - se os temas do Microsoft Windows estão ativados ou desativados.
- Se a conexão automática com o desktop remoto está ativada ou desativada:
 - senha para conexão com o desktop remoto, somente se a opção para conectar automaticamente estiver selecionada.
- Configurações da conexão RDP do thin client:
 - certificado do servidor RDP;
 - segredo;
 - modo de conexão do desktop remoto do thin client (automático, confirmação do usuário ou negado);
 - modo de exibição de conteúdo remoto (automático, confirmação do usuário ou desativado).
- Configurações de rede:
 - se a configuração automática de rede via DHCP está ativada ou desativada;
 - endereço IP do thin client;
 - máscara de sub-rede;
 - lista de endereços IP de servidores DNS;
 - endereço IP do gateway de rede.
- Configurações de economia de energia: número de minutos antes que o monitor seja desativado e o número de minutos antes que o thin client seja desativado quando o Kaspersky Thin Client estiver ocioso.
- Configurações de conexão do servidor de log:
 - endereço (nome ou endereço IP e porta) do servidor de log usado para encaminhar os logs de auditoria e de eventos;
 - arquivos de certificado para autenticar o servidor de log quando o Kaspersky Thin Client se conecta a esse servidor.

- Configurações de data e hora:
 - data e hora de recebimento do Servidor de Administração durante a última sincronização com o Kaspersky Security Center;
 - fuso horário.
- Informações sobre as atualizações disponíveis e baixadas pelo Kaspersky Thin Client:
 - status de disponibilidade da atualização;
 - status de instalação da atualização;
 - status de entrega da atualização;
 - dados da atualização disponível: versão do Kaspersky Thin Client, nome da versão, data e hora, importância;
 - hora da última verificação de atualização bem-sucedida;
 - hora da última instalação de atualização bem-sucedida.
- Informações sobre os Contratos de Licença de Usuário Final do Kaspersky Thin Client:
 - IDs do Contrato de Licença de Usuário Final;
 - Contratos de Licença de Usuário Final em russo, inglês, espanhol e português do Brasil;
 - informações quanto à aceitação ou não aceitação dos Contratos de Licença de Usuário Final;
 - informações sobre as datas de lançamento dos Contratos de Licença de Usuário Final.

Qualquer informação recebida é protegida pela Kaspersky de acordo com os requisitos estabelecidos por lei e de acordo com os regulamentos atuais da Kaspersky. Os dados são transmitidos pelos canais de comunicação criptografados.

Primeira ativação do Kaspersky Thin Client

Antes de começar a trabalhar com o Kaspersky Thin Client, é preciso conectar um mouse, um teclado e um monitor ao thin client pelas portas correspondentes. O Kaspersky Thin Client também é compatível com a conexão [de dispositivos periféricos](#) enquanto o sistema está em execução.

Este documento não fornece uma visão geral dos componentes de hardware de um thin client (incluindo controles e conectores), pois essas informações já são fornecidas na documentação do fornecedor do dispositivo. Para descobrir os modelos específicos de thin clients em que o Kaspersky Thin Client pode ser instalado, consulte a [seção com informações básicas sobre o Kaspersky Thin Client](#).

Para começar a trabalhar com o Kaspersky Thin Client, é necessário ativar o thin client.

Para ativar o Kaspersky Thin Client e concluir o primeiro procedimento de inicialização:

1. Pressione o botão liga/desliga no thin client.

O Kaspersky Thin Client começará a ser carregado no seu dispositivo. Após o sistema ser carregado, ele exibirá uma janela de seleção de idioma da interface do usuário.

2. Selecione o idioma da interface desejado e clique em **Avançar**.

Uma janela se abre com o texto do [Contrato de Licença de Usuário Final](#) no idioma selecionado.

3. Leia atentamente o texto do Contrato de Licença de Usuário Final e clique em **Aceitar**.

Caso você não aceite os termos e as condições do Contrato de Licença de Usuário Final, você deve cancelar a inicialização do Kaspersky Thin Client e parar de usar o aplicativo.

Agora, a inicialização foi concluída e o [desktop](#) do Kaspersky Thin Client é exibido.

Ao ligar o thin client novamente, o desktop é exibido após o carregamento do sistema.

Reiniciar e desativar o Kaspersky Thin Client

Ao concluir o trabalho com o Kaspersky Thin Client, é necessário desativar o thin client.

Para desativar o Kaspersky Thin Client:

1. No painel de controle do desktop do Kaspersky Thin Client, clique no botão de desligamento .
2. No menu que se abre, selecione **Encerrar**.

O Kaspersky Thin Client será desativado.

É possível reiniciar o Kaspersky Thin Client caso necessário. Por exemplo, se for necessário aplicar o idioma selecionado para a interface do Kaspersky Thin Client ou instalar atualizações do sistema.

Para reiniciar o Kaspersky Thin Client:

1. No painel de controle do desktop do Kaspersky Thin Client, clique no botão de desligamento .
2. No menu aberto, selecione **Reiniciar**.

O Kaspersky Thin Client será reiniciado.

Uso de certificados no Kaspersky Thin Client

O [protocolo de criptografia TLS](#) garante a transferência segura de dados entre um cliente e um servidor usando certificados de conexão SSL. Um *certificado de conexão SSL* (também chamado de “certificado SSL” ou simplesmente “certificado”) é um bloco de dados contendo informações sobre o proprietário do certificado, a chave pública do proprietário e as datas de início e fim de validade do certificado.

No Kaspersky Thin Client, os certificados são usados para as seguintes finalidades:

- [Conexão de um thin client ao Kaspersky Security Center](#).
- Conexão com um ambiente remoto:
 - autenticação do servidor do Remote Desktop Connection Broker ao se conectar com um desktop remoto ou aplicativo virtual
 - autenticação do broker ao se conectar com um desktop remoto gerenciado pelo Basis.WorkPlace
 - autenticação do endereço do servidor ao se conectar com um ambiente remoto no Web Access
- Conexão a um servidor de log.

O usuário pode [aceitar ou rejeitar independentemente um certificado na interface do Kaspersky Thin Client](#) se as seguintes condições forem atendidas:

- O usuário está se conectando a um [ambiente remoto](#) ou a um [servidor de log](#) na interface do Kaspersky Thin Client pela primeira vez.
- O thin client está em um dos seguintes estados:
 - não conectado ao Kaspersky Security Center
 - não adicionado ao grupo de administração
 - [nenhum certificado para conexão ao ambiente remoto foi adicionado](#) para o grupo de administração ao qual o thin client pertence

Todos os certificados aceitos serão salvos no armazenamento de certificados do thin client. Nesse caso, um usuário também pode se conectar a nós e usar certificados que não são controlados pelo administrador.

Nós recomendamos [configurar a conexão do Kaspersky Thin Client](#) com um servidor de log e com um ambiente remoto usando somente certificados que foram atribuídos pelo administrador no Web Console. Nesse caso, todos os certificados que foram aceitos anteriormente por um usuário serão removidos do armazenamento de certificados do thin client. Essas medidas ajudarão a impedir que o Kaspersky Thin Client se conecte a nós não confiáveis.

Recomendamos atualizar os certificados atribuídos nos seguintes casos:

- Os certificados atuais foram comprometidos.
- Os certificados expiraram.
- Os certificados precisam ser atualizados regularmente de acordo com os requisitos de segurança de informações de sua empresa.

O Kaspersky Thin Client não verifica se o certificado está na lista de revogação de certificados.

Configuração do Kaspersky Thin Client

Esta seção descreve como configurar o Kaspersky Thin Client.

Cenário: início rápido para administradores

Esta seção descreve a sequência de etapas que devem ser executadas para configurar o Kaspersky Thin Client e o Kaspersky Security Center, e para estabelecer uma conexão entre eles. Essas etapas devem ser executadas pelo administrador ou outro especialista qualificado de sua empresa, que possa verificar a autenticidade do certificado aceito e usado para se conectar ao Kaspersky Security Center.

As instruções sobre a instalação do Kaspersky Thin Client em um thin client são fornecidas em um [artigo separado](#).

Antes da instalação do Kaspersky Thin Client ou antes da primeira inicialização de um thin client no qual um sistema Kaspersky Thin Client está pré-instalado, é recomendável atualizar o BIOS no thin client para a versão mais recente, definir uma senha para alterações de configuração do BIOS e configurar a opção para inicializar somente a partir de um dispositivo SSD local. Essas medidas recomendadas ajudarão a evitar possíveis riscos de segurança, como substituição do sistema operacional, substituição ou exclusão de certificados de conexão do servidor remoto e acesso não autorizado às configurações do sistema operacional.

O Kaspersky Thin Client é compatível com a tecnologia Secure Boot que permite à UEFI verificar a autenticidade dos componentes carregados. Caso queira configurar a Inicialização segura, será possível obter as chaves necessárias com os especialistas da Kaspersky, e, além disso, usar as instruções da [Base de conhecimento](#).

O cenário para a configuração inicial do Kaspersky Thin Client e do Kaspersky Security Center e para o estabelecimento de uma conexão entre eles consiste nas seguintes etapas:

1 Instalação do Kaspersky Security Center

Baixe o pacote de distribuição do Kaspersky Security Center e instale a versão completa do Kaspersky Security Center no servidor. O pacote de distribuição da versão completa do Kaspersky Security Center inclui o Kaspersky Security Center Web Console. Recomendamos selecionar a instalação padrão. Para obter detalhes sobre a instalação do Kaspersky Security Center, consulte a [Ajuda on-line do Kaspersky Security Center](#).

2 Configuração das regras de firewall

Caso queira usar a porta padrão para conectar o thin client ao Kaspersky Security Center, defina as regras que permitem conexões TCP pela porta 13292 para o firewall do sistema operacional do servidor no qual o Kaspersky Security Center está instalado. Caso queira usar uma porta diferente da 13292, defina as permissões adequadamente. Para obter informações detalhadas quanto à configuração das regras de firewall, consulte a documentação do sistema operacional usado.

3 Instalação do plug-in da Web do Kaspersky Security Management Suite

No Kaspersky Security Center Web Console, instale o [plug-in da Web do Kaspersky Security Management Suite](#).

4 Preparação das portas

O Kaspersky Thin Client usa um protocolo móvel para conexão com o Kaspersky Security Center. No Servidor de Administração do Kaspersky Security Center, ative o uso da porta TCP à qual o acesso na etapa 2 foi configurado. Para obter mais informações sobre a ativação de uma porta TCP no Servidor de Administração do Kaspersky Security Center, consulte a [Ajuda on-line do Kaspersky Security Center](#).

5 Ativação do Kaspersky Thin Client

[Ative o Kaspersky Thin Client](#) e aguarde o carregamento do sistema. Selecione o idioma do sistema. Leia os termos e as condições do Contrato de Licença de Usuário Final e aceite o contrato.

6 Definição das configurações do Kaspersky Thin Client

Depois de ativar o Kaspersky Thin Client e aceitar o Contrato de Licença de Usuário Final, defina as [configurações gerais](#) e as [configurações de conexão de rede](#).

7 Configuração de uma conexão entre o Kaspersky Thin Client e o Kaspersky Security Center

Na interface do Kaspersky Thin Client, [configure a conexão com o Kaspersky Security Center](#).

8 Adição de um thin client que executa o Kaspersky Thin Client a um grupo de administração

No Web Console, [adicione o thin client ao grupo de administração](#) de forma manual ou configure a transferência automatizada de dispositivos.

9 Criação de uma política ativa no Kaspersky Security Center

Na interface do Web Console, [crie uma política ativa](#) para o grupo de administração.

10 Atribuição de certificados para um grupo de administração

[Atribua certificados](#) para conectar um grupo de administração a um ambiente remoto e a um servidor de log. Também recomendamos [adicionar um certificado](#) para conectar o Kaspersky Thin Client ao Kaspersky Security Center.

Quando essas ações forem concluídas, o sistema do Kaspersky Thin Client estará pronto para operação. Será possível controlar o Kaspersky Thin Client pela interface do sistema ou pelo Kaspersky Security Center Web Console, bem como monitorar eventos do Kaspersky Thin Client.

Cenário: atribuição de certificado para um grupo de thin clients

Se os certificados forem atribuídos a um [grupo de administração](#) no Kaspersky Security Center Web Console, um usuário de um thin client incluído nesse grupo poderá se conectar somente aos servidores para os quais os certificados foram adicionados no Web Console.

[O Kaspersky Security Center deve ser instalado e configurado](#) com antecedência.

O cenário para atribuir certificados a um grupo de thin clients inclui as seguintes etapas:

1 Configuração de uma conexão com o Kaspersky Security Center

Na interface do Kaspersky Thin Client, [configure a conexão com o Kaspersky Security Center](#).

2 Adição de thin clients ao grupo de administração

Na interface do Web Console, [adicione um thin client ao grupo de administração](#) caso o thin client ainda esteja no grupo de dispositivos não atribuídos.

3 Criação de uma política ativa do Kaspersky Security Center para o Kaspersky Thin Client

Na interface do Web Console, [crie uma política ativa](#) para o grupo de administração pertinente.

4 Adição de certificados para conexão a um ambiente remoto e a um servidor de log

Na interface do Kaspersky Security Center Web Console, [adicione certificados exigidos](#) e mova o botão de alternância na parte direita da página para a posição **Aplicado**. Aguarde até que o Kaspersky Thin Client seja totalmente sincronizado com o Kaspersky Security Center. É possível definir o período de sincronização ao configurar o Kaspersky Thin Client pelo Kaspersky Security Center Web Console. Após a sincronização, os dispositivos receberão os certificados do Servidor de Administração do Kaspersky Security Center.

Se você [remover todos os certificados](#) que foram atribuídos a um grupo de dispositivos, os usuários de thin clients desse grupo poderão se conectar a qualquer servidor, incluindo servidores aos quais nenhum certificado foi atribuído.

Cenário: migração de thin client para um novo servidor do Kaspersky Security Center

Esta seção descreve as etapas a serem executadas pelo administrador ao configurar dispositivos que executam o Kaspersky Thin Client para gerenciamento por meio de um novo Servidor de Administração do Kaspersky Security Center (aqui também referido como "o Servidor") caso esses dispositivos tenham sido anteriormente gerenciados por um servidor do Kaspersky Security Center diferente.

O cenário para configurar o gerenciamento do Kaspersky Thin Client ao migrar thin clients para um novo servidor do Kaspersky Security Center consiste nas seguintes etapas:

1 Instalação de um novo Servidor de Administração do Kaspersky Security Center

Baixe o pacote de distribuição do Kaspersky Security Center e instale a versão completa do Kaspersky Security Center no servidor. O pacote de distribuição da versão completa do Kaspersky Security Center inclui o Kaspersky Security Center Web Console. Recomendamos selecionar a instalação padrão. Para obter detalhes sobre a instalação do Kaspersky Security Center, consulte a [Ajuda on-line do Kaspersky Security Center](#).

2 Configuração das regras de firewall

Caso queira usar a porta padrão para conectar o thin client ao Kaspersky Security Center, defina as regras que permitem conexões TCP pela porta 13292 para o firewall do sistema operacional do servidor no qual o Kaspersky Security Center está instalado. Caso queira usar uma porta diferente da 13292, defina as permissões adequadamente. Para obter informações detalhadas quanto à configuração das regras de firewall, consulte a documentação do sistema operacional usado.

3 Instalação do plug-in da Web do Kaspersky Security Management Suite

No Web Console, instale o [plug-in da Web do Kaspersky Security Management Suite](#) para o novo Servidor de Administração do Kaspersky Security Center.

4 Preparação das portas

O Kaspersky Thin Client usa um protocolo móvel para conexão com o Kaspersky Security Center. No Servidor de Administração do Kaspersky Security Center, ative o uso da porta TCP à qual o acesso na etapa 2 foi configurado. Para obter mais informações sobre a ativação de uma porta TCP no Servidor de Administração do Kaspersky Security Center, consulte a [Ajuda on-line do Kaspersky Security Center](#).

5 Ativação do Kaspersky Thin Client

[Ative o Kaspersky Thin Client](#) e aguarde o carregamento do sistema.

6 Criação de uma política ativa do Kaspersky Security Center para o Kaspersky Thin Client

No Web Console usado anteriormente, [crie uma política ativa para o grupo de dispositivos](#) que será gerenciado por meio do novo servidor do Kaspersky Security Center.

7 Atualização do certificado de segurança para conexão com o Kaspersky Security Center

[Emita um certificado](#) que precisa ser salvo como reserva no Servidor de Administração atual do Kaspersky Security Center e, em seguida, usado no novo servidor como certificado principal.

8 Configuração de uma conexão entre o Kaspersky Thin Client e o servidor do novo Kaspersky Security Center

Caso um servidor DHCP seja implementado na infraestrutura da empresa e as configurações para conectar o Kaspersky Thin Client ao Kaspersky Security Center sejam recebidas automaticamente, use a opção 224 para definir o endereço IP ou o nome de domínio do novo Servidor de Administração do Kaspersky Security Center e aguarde até que todos os dispositivos executem o Kaspersky Thin Client para concluir a sincronização com o Kaspersky Security Center.

Caso um servidor DHCP não esteja implementado na infraestrutura da empresa, [configure manualmente a conexão ao novo Kaspersky Security Center na interface do Kaspersky Thin Client](#).

Os grupos de administração de thin client são conectados ao novo servidor do Kaspersky Security Center e é possível gerenciá-los com o uso da interface do Web Console.

Definição das configurações gerais

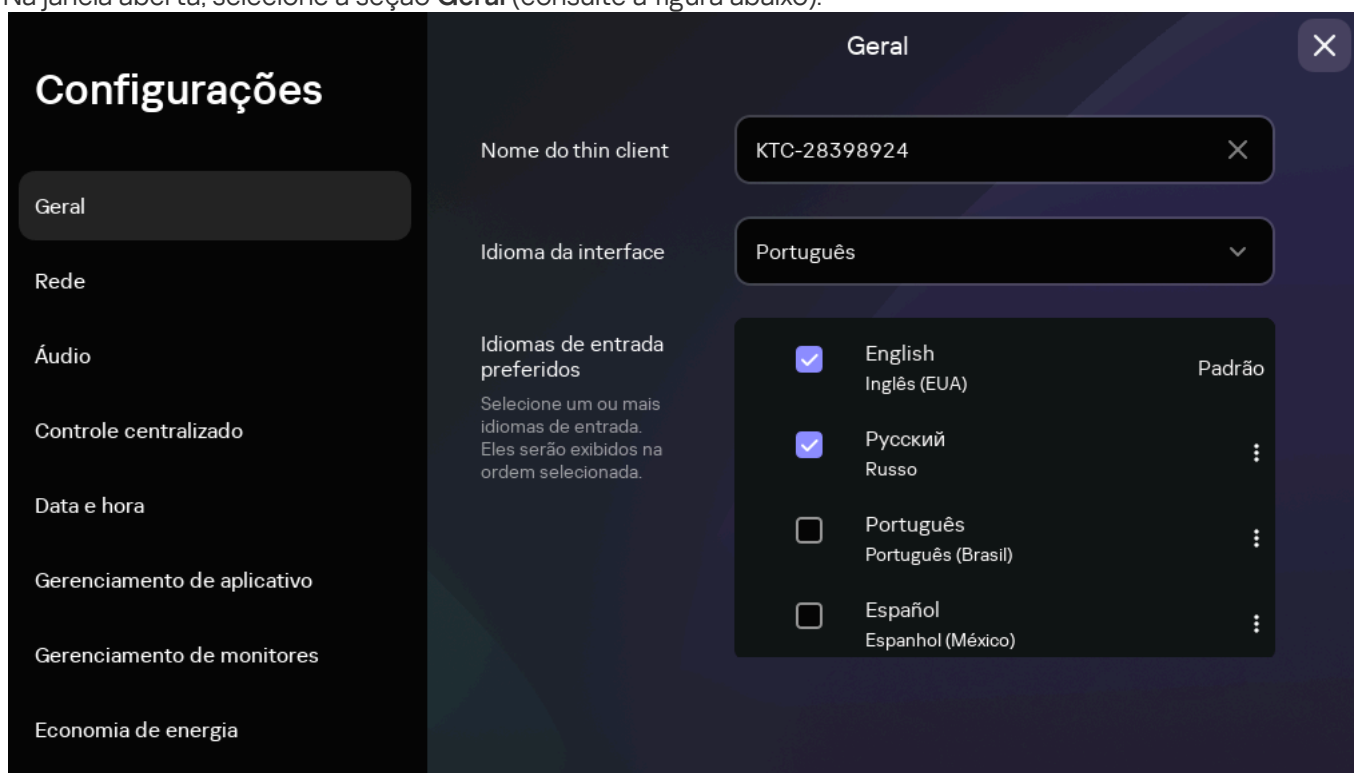
Na interface do Kaspersky Thin Client, é possível definir as configurações gerais do thin client. Por exemplo, é possível especificar o nome do thin client que será exibido na barra de tarefas do Kaspersky Thin Client e no Kaspersky Security Center Web Console, além de selecionar o idioma da interface do Kaspersky Thin Client.

Se o thin client estiver incluído em um [grupo de administração](#), os valores das configurações especificadas neste artigo poderão ser aplicados pelo Web Console. Se for esse o caso, não será possível definir essas configurações na interface do Kaspersky Thin Client.

As configurações especificadas neste artigo podem estar [ocultas no Kaspersky Thin Client](#).

Para definir as configurações gerais do Kaspersky Thin Client:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Geral** (consulte a figura abaixo).



Configurações. Seção Geral

3. No campo **Nome do thin client**, insira o nome que será exibido para o Kaspersky Thin Client no Web Console. O nome pode conter letras maiúsculas e minúsculas dos alfabetos latino e cirílico, numerais e um hífen. O comprimento do nome do thin client não deve exceder 30 caracteres.
4. Na lista **Idioma da interface**, selecione um idioma da interface do usuário. O Kaspersky Thin Client 2.3 é compatível com os seguintes idiomas de interface: russo, inglês (EUA), espanhol (México) e português (Brasil).
5. Na lista suspensa **Idiomas de entrada preferidos**, selecione um ou mais idiomas. O Kaspersky Thin Client é compatível com os seguintes idiomas de entrada: inglês (EUA), russo, espanhol (México), alemão (padrão e suíço), português (Brasil) e francês (Suíça). Os idiomas selecionados são exibidos no painel de controle do Kaspersky Thin Client na ordem selecionada e estão disponíveis com a alternância do idioma de entrada do teclado.

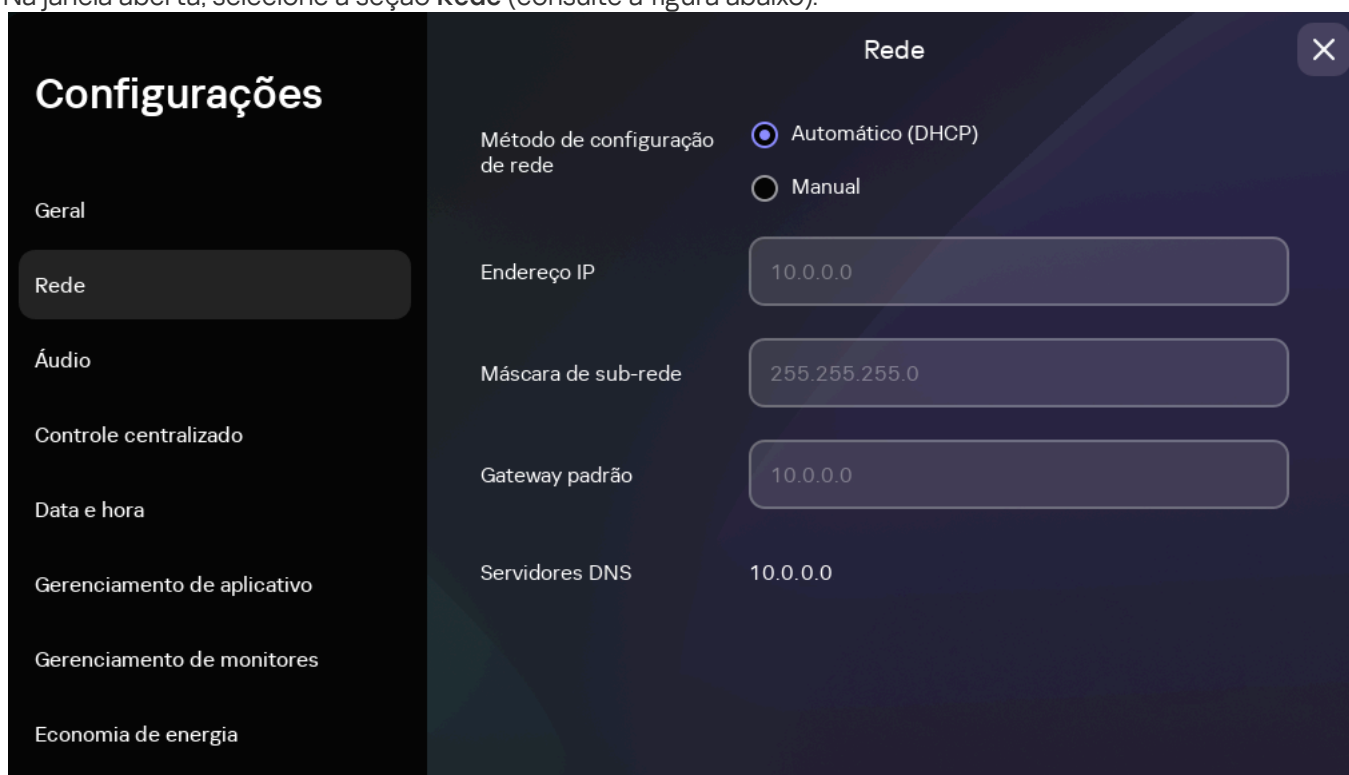
As alterações serão aplicadas após o [thin client ser reiniciado](#).

Definição das configurações de rede

Na interface do Kaspersky Thin Client, é possível definir as configurações para conectar o Kaspersky Thin Client à rede.

Para definir as configurações de rede:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Rede** (consulte a figura abaixo).



Configurações. Seção Rede

3. Defina as configurações para conectar o Kaspersky Thin Client à rede:

- Caso seja necessário receber as configurações de rede automaticamente via DHCP, selecione **Automático (DHCP)** para o parâmetro **Método de configuração de rede**. Nesse modo, os campos **Endereço IP**, **Máscara de sub-rede**, **Gateway padrão** e **Servidores DNS** não estão acessíveis.
- Caso seja necessário especificar as configurações de rede manualmente, selecione **Manual** para o parâmetro **Método de configuração de rede** e faça o seguinte:
 - No campo **Endereço IP**, insira o endereço IP do Kaspersky Thin Client no formato IPv4.
 - No campo **Máscara de sub-rede**, insira a máscara de sub-rede.
 - No campo **Gateway padrão**, insira o endereço do gateway de rede.
 - No campo **Servidores DNS**, insira os endereços dos servidores DNS. Não é possível inserir mais de dois endereços.

4. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

Gerenciamento de dispositivos de reprodução e gravação de áudio

É possível conectar diversos dispositivos de reprodução e gravação de áudio a um thin client que executa o Kaspersky Thin Client por um miniconector ou uma porta USB para redirecioná-los ao ambiente remoto. Na interface do Kaspersky Thin Client, é possível [alternar entre dispositivos conectados](#).

O volume do áudio e outras configurações são gerenciados no ambiente remoto.

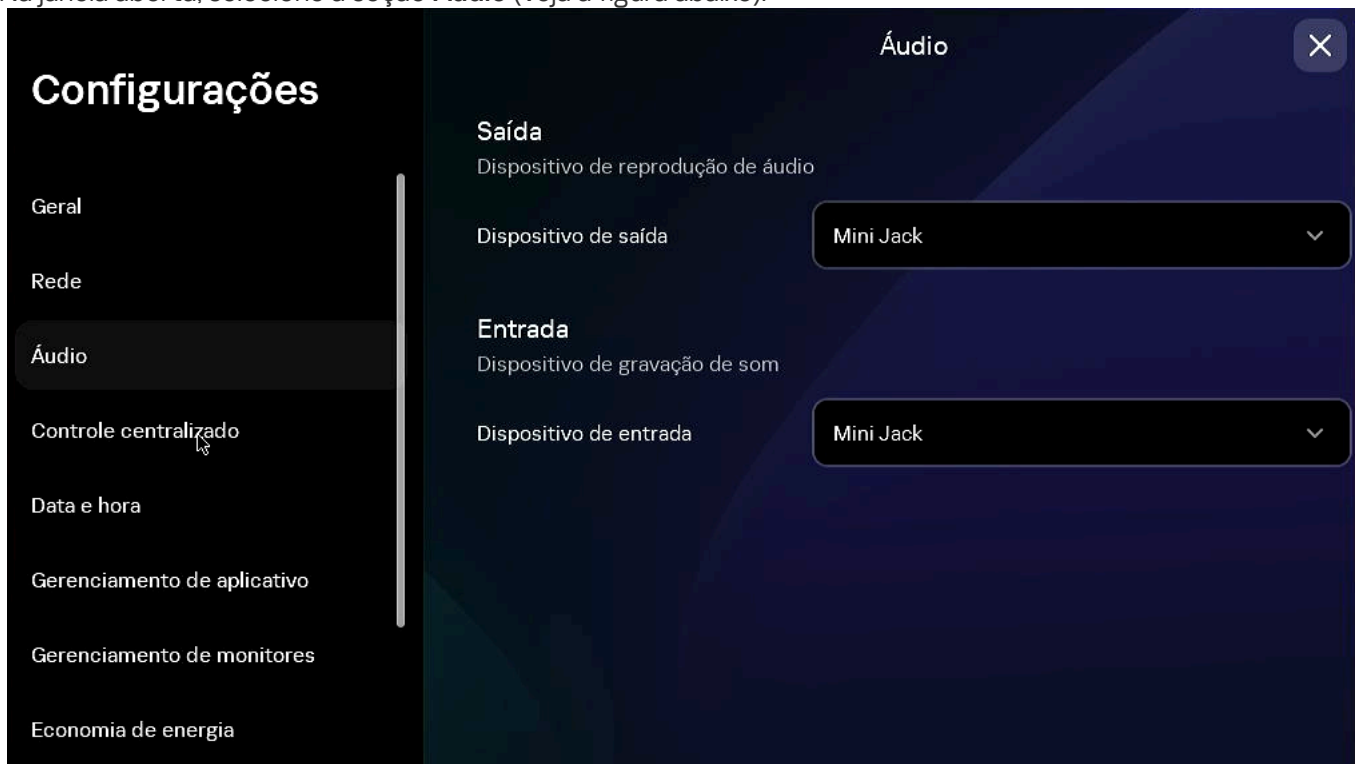
A conexão por meio de miniconector não é compatível com thin clients Dell Wyse 3040.

Se o thin client estiver incluído em um [grupo de administração](#), os valores das configurações especificadas neste artigo poderão ser aplicados pelo Web Console. Se for esse o caso, não será possível definir essas configurações na interface do Kaspersky Thin Client.

As configurações especificadas neste artigo podem estar [ocultas no Kaspersky Thin Client](#).

Para selecionar dispositivos de reprodução e gravação de áudio no Kaspersky Thin Client:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Áudio** (veja a figura abaixo).



Configurações. Seção Áudio

3. Na lista suspensa **Dispositivo de saída**, selecione o dispositivo de reprodução de áudio.
4. Na lista suspensa **Dispositivo de entrada**, selecione o dispositivo de gravação de áudio.

Também é possível usar dispositivos de reprodução e gravação de áudio no ambiente remoto e [alternar entre eles no painel de conexão](#).

Definição das configurações de conexão do Kaspersky Thin Client com o Kaspersky Security Center

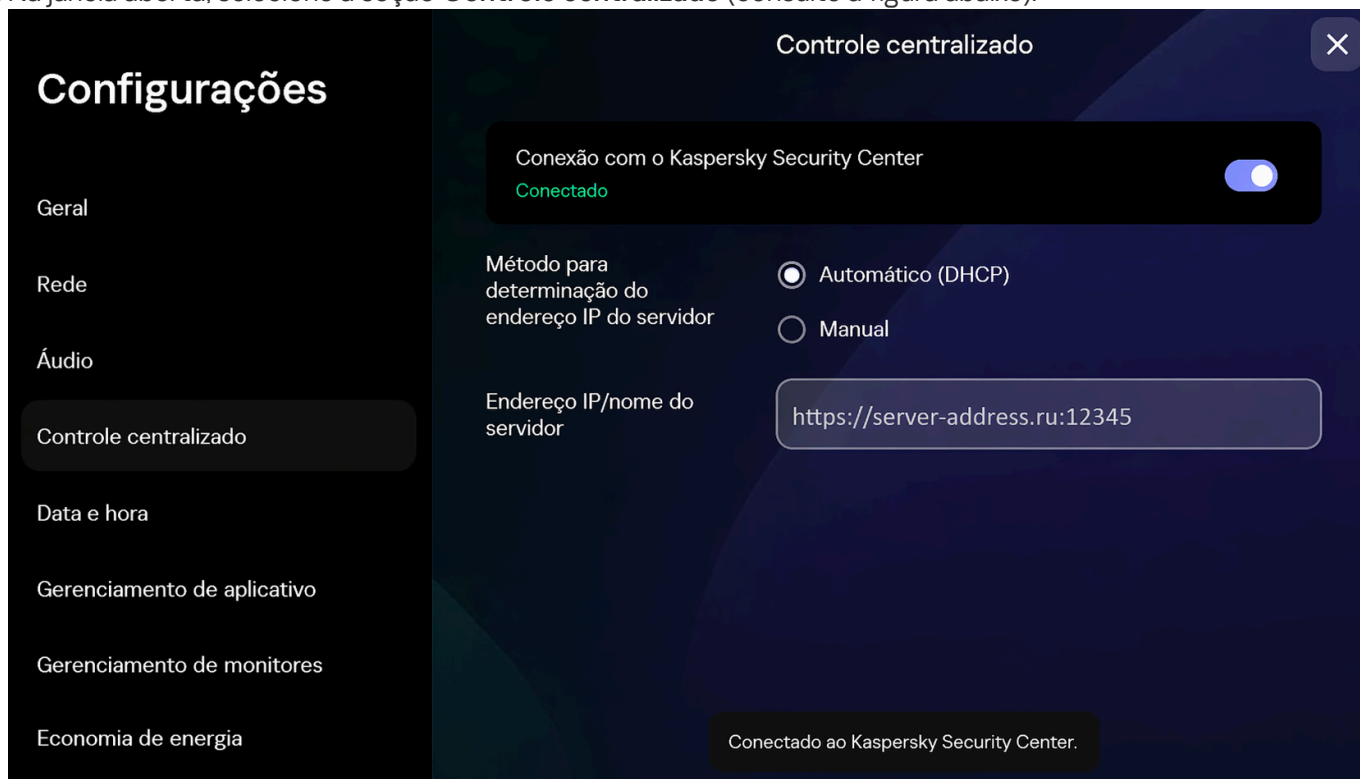
Para gerenciar um thin client pelo Web Console, é necessário definir as configurações para conectar o Kaspersky Thin Client ao Servidor de Administração do Kaspersky Security Center (a seguir também designado apenas como "Kaspersky Security Center").

Recomendamos configurar a conexão do Kaspersky Thin Client ao Kaspersky Security Center com a ajuda de um dos especialistas qualificados de sua empresa, que poderá verificar a autenticidade do certificado aceito.

Recomendamos usar um Servidor de Administração do Kaspersky Security Center separado para gerenciar thin clients e receber atualizações de segurança importantes dos servidores de atualização da Kaspersky. O motivo é que um Servidor de Administração do Kaspersky Security Center pode ter apenas uma [tarefa de atualização](#) ativa com uma fonte de atualização prioritária.

Para definir as configurações para conectar o Kaspersky Thin Client ao Servidor de Administração do Kaspersky Security Center:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Controle centralizado** (consulte a figura abaixo).



Configurações. Seção Controle centralizado

3. Na janela aberta **Controle centralizado**, defina as seguintes configurações para conectar o Kaspersky Thin Client ao Kaspersky Security Center:

- Caso queira usar o protocolo DHCP para receber automaticamente as configurações para conectar o Kaspersky Thin Client ao Kaspersky Security Center, selecione **Automático (DHCP)** em **Método para determinação do endereço IP do servidor**. Nesse modo, o campo **Endereço IP/nome do servidor** não pode ser editado.

Para usar essa opção de conexão, um servidor DHCP deve ser implementado na infraestrutura corporativa e a opção 224 deve ser usada para definir o endereço IP ou o nome de domínio do Servidor de Administração do Kaspersky Security Center ao qual o usuário planeja conectar o Kaspersky Thin Client. O Kaspersky Thin Client recebe valores de string em **Endereço IP:formato da porta** ou **Nome do servidor:formato da porta** na opção 224. Por exemplo, 192.168.2.4 ou ksc.exemplo.com:12345. A porta deve ser especificada apenas se uma porta diferente da porta 13292 for usada para a conexão.

Por padrão, o uso do DHCP é ativado para receber automaticamente as configurações para conectar o Kaspersky Thin Client ao Kaspersky Security Center.

- Caso queira definir manualmente as configurações para conectar o Kaspersky Thin Client ao Kaspersky Security Center, selecione **Manual** no **Método para determinação do endereço IP do servidor** e no campo **Endereço IP/nome do servidor** insira o endereço IP ou o nome do Servidor de Administração do Kaspersky Security Center. Caso esteja usando uma porta diferente da porta 13292, indique-a em **Endereço IP:formato da porta** ou **Nome do servidor:formato da porta**.

4. Ative o botão de alternância **Conexão com o Kaspersky Security Center**.

5. Caso esteja se conectando ao Kaspersky Security Center pela primeira vez, verifique as configurações do certificado usado para conectar o Kaspersky Thin Client ao Kaspersky Security Center na janela **Adicionar certificado** e clique no botão **Adicionar certificado**. O certificado adicionado será usado para conexões subsequentes entre o Kaspersky Thin Client e o Kaspersky Security Center.

Caso o certificado usado para conectar o Kaspersky Thin Client ao Kaspersky Security Center tenha sido alterado no Kaspersky Security Center, será necessário [confirmar a alteração do certificado](#) para continuar a configurar a conexão.

O Kaspersky Thin Client tentará se conectar ao Kaspersky Security Center. Após a conexão bem-sucedida com o Kaspersky Security Center, o status **Conectado ao Kaspersky Security Center** será exibido.

Alteração das configurações para conectar o Kaspersky Thin Client ao Kaspersky Security Center

Se o thin client estiver incluído em um [grupo de administração](#), os valores das configurações especificadas neste artigo poderão ser aplicados pelo Web Console. Se for esse o caso, não será possível definir essas configurações na interface do Kaspersky Thin Client.

As configurações especificadas neste artigo podem estar [ocultas no Kaspersky Thin Client](#).

Para alterar as configurações para conectar o Kaspersky Thin Client ao Kaspersky Security Center:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Controle centralizado**.

3. Desative o botão de alternância **Conexão com o Kaspersky Security Center**.
4. Na janela aberta **Confirmar desconexão**, visualize e memorize o código de confirmação para desconectar o Kaspersky Thin Client do Kaspersky Security Center, então, forneça-o ao administrador do Kaspersky Security Center. Os detalhes de contato do administrador são fornecidos na janela **Confirmar desconexão**. O administrador deve enviar um código de confirmação para você como resposta.
5. Clique em **Avançar**.
6. Na janela aberta **Código de confirmação**, insira o código fornecido pelo administrador do Kaspersky Security Center e clique no botão **Confirmar**.
O Kaspersky Thin Client será desconectado do gerenciamento pelo Kaspersky Security Center.
7. Na janela de **Controle centralizado**, defina manualmente [as configurações para conexão com o Kaspersky Security Center](#).
8. Ative o botão de alternância **Conexão com o Kaspersky Security Center**.
O thin client tentará se conectar com o Kaspersky Security Center. Após a conexão bem-sucedida com o Kaspersky Security Center, o status **Conectado ao Kaspersky Security Center** será exibido.

Configuração da data e a hora

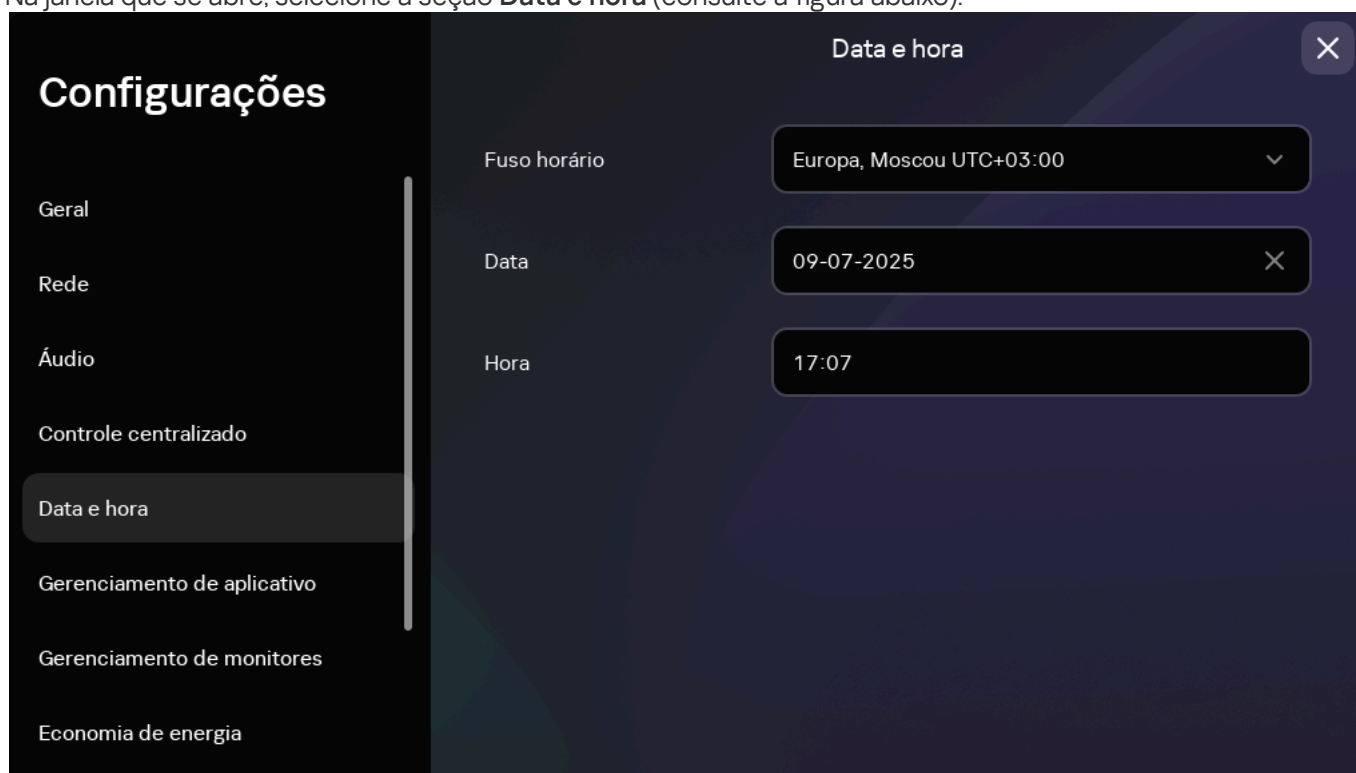
Quando um thin client está conectado ao Kaspersky Security Center, ele recebe a data e hora do Servidor de Administração do Kaspersky Security Center. É possível alterar manualmente a data e hora do Kaspersky Thin Client apenas se o sistema não estiver sendo controlado pelo Kaspersky Security Center.

Se o thin client estiver incluído em um [grupo de administração](#), os valores das configurações especificadas neste artigo poderão ser aplicados pelo Web Console. Se for esse o caso, não será possível definir essas configurações na interface do Kaspersky Thin Client.

As configurações especificadas neste artigo podem estar [ocultas no Kaspersky Thin Client](#).

Para alterar a data e a hora do Kaspersky Thin Client:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela que se abre, selecione a seção **Data e hora** (consulte a figura abaixo).



Configurações. Seção Data e hora

3. Defina as configurações de data e hora:
 - Selecione o fuso horário pertinente a partir da lista suspensa **Fuso horário**.
 - No campo **Data**, insira a data atual no formato DD-MM-AAAA.
 - No campo **Hora**, insira a hora atual no formato HH:MM:SS.
4. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

Configuração da inicialização automática e exibição de aplicativos

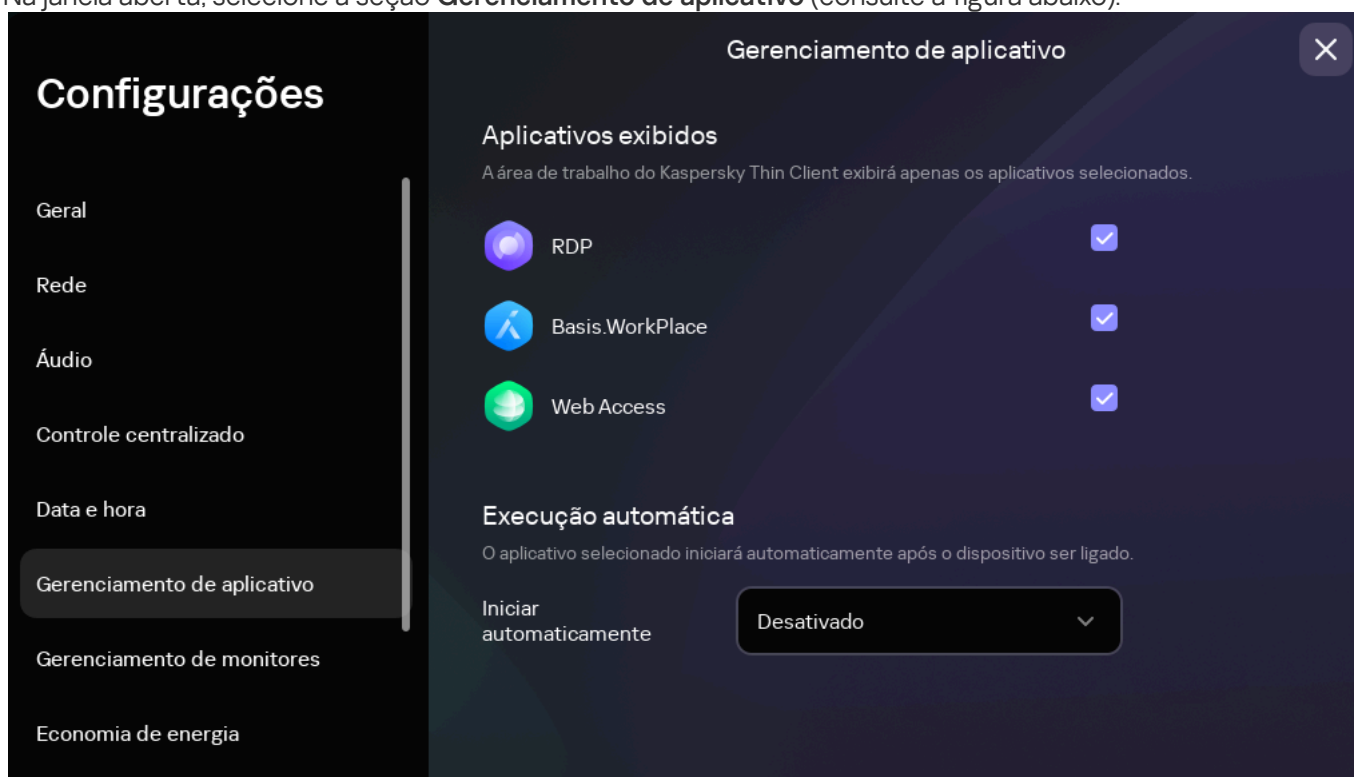
É possível selecionar um [aplicativo](#) que será iniciado automaticamente após iniciar o dispositivo e inicializar o sistema, e também é possível especificar quais aplicativos serão exibidos no Desktop do Kaspersky Thin Client.

Se o thin client estiver incluído em um [grupo de administração](#), os valores das configurações especificadas neste artigo poderão ser aplicados pelo Web Console. Se for esse o caso, não será possível definir essas configurações na interface do Kaspersky Thin Client.

As configurações especificadas neste artigo podem estar [ocultas no Kaspersky Thin Client](#).

Para configurar a inicialização automática e a exibição de aplicativos:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Gerenciamento de aplicativo** (consulte a figura abaixo).



Configurações. Seção Gerenciamento de aplicativo

3. No bloco **Aplicativos exibidos**, marque as caixas de seleção ao lado dos aplicativos que serão exibidos no Desktop do Kaspersky Thin Client.
4. Na lista suspensa **Iniciar automaticamente**, selecione o aplicativo que será iniciado automaticamente após ligar o dispositivo e inicializar o sistema. Caso selecione **Desativado**, a inicialização automática será desativada.

As alterações serão salvas e aplicadas.

Também é possível [configurar a conexão automática a um ambiente remoto no aplicativo RDP](#) para iniciar uma sessão remota após inicializar o Kaspersky Thin Client.

Configuração de monitores e telas

O Kaspersky Thin Client é compatível com a conexão de dois monitores.

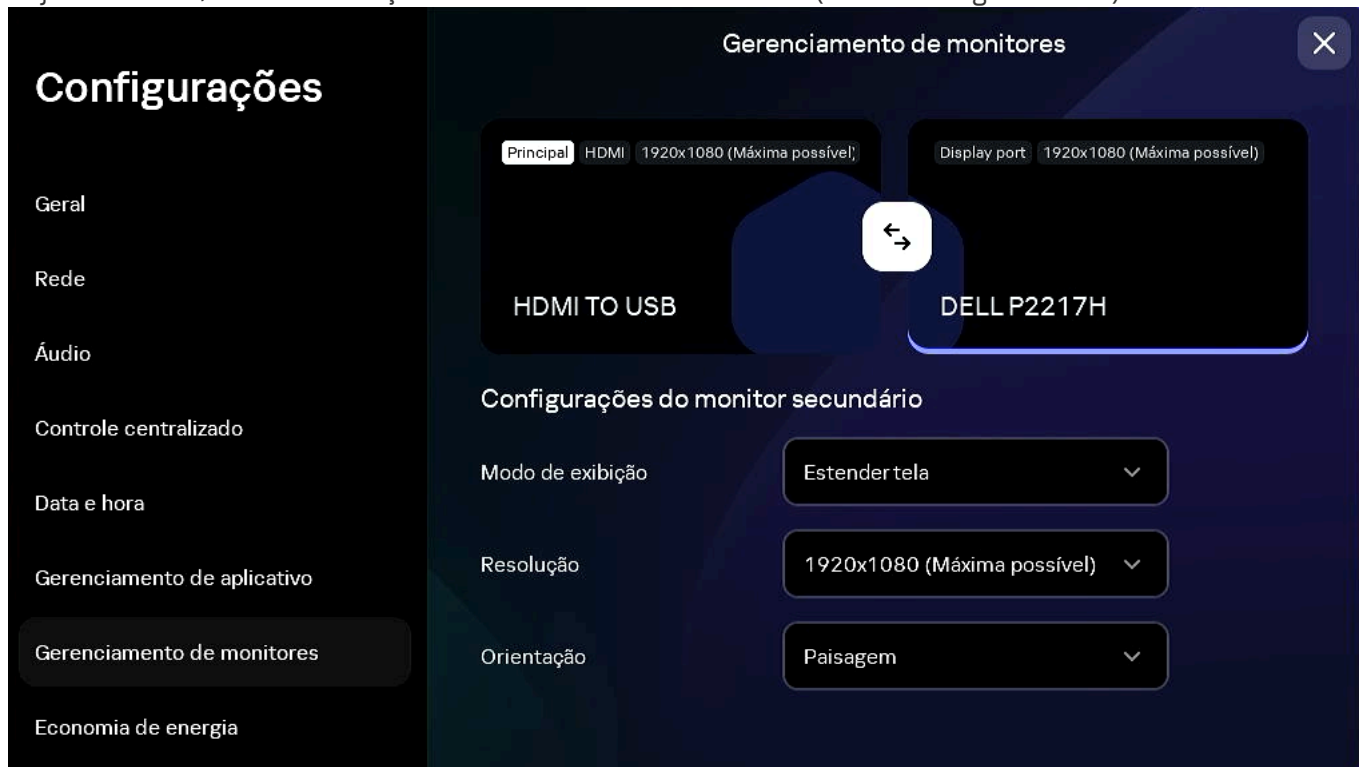
Quando dois monitores são conectados, o sistema considera um como sendo o principal e o outro como secundário. Durante uma [sessão remota](#), o painel de conexão é exibido na tela do monitor principal. A tela do monitor secundário estende ou duplica a imagem do monitor principal. Na interface do Kaspersky Thin Client, é possível selecionar qual monitor será considerado como principal (doravante também "alterar o layout do monitor").

Se você quiser que a tela da sessão remota seja exibida em ambos os monitores, ative essa opção nas configurações de conexão do ambiente remoto nos aplicativos [RDP](#) ou [Basis.WorkPlace](#).

Na interface do Kaspersky Thin Client, é possível visualizar informações sobre monitores conectados ao thin client e alterar o layout de exibição das telas, assim como definir as configurações para cada um dos monitores.

Para configurar monitores e telas:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Gerenciamento de monitores** (consulte a figura abaixo).



Configurações. Seção Gerenciamento de monitores

3. Se houver dois monitores conectados ao thin client, será possível alterar o layout deles. Para fazer isso, clique no  botão.

4. Se você quiser personalizar a tela de um monitor específico, selecione o monitor. Para fazer isso, clique na imagem esquemática.

Para destacar o monitor que será personalizado, passe o mouse sobre a imagem esquemática dos monitores. Uma moldura vermelha aparecerá na imagem personalizada do monitor.

5. Defina as configurações necessárias:

- Na lista suspensa **Modo de exibição**, selecione a opção de exibição de imagem:
 - **Estender tela:** a imagem se estenderá por dois monitores.
 - **Duplicar tela:** a imagem da tela do monitor principal será duplicada no monitor secundário. Se essa opção for selecionada, as configurações listadas abaixo não estarão disponíveis para a exibição adicional.

Essa opção só será exibida se dois monitores estiverem conectados ao thin client.

- Na lista suspensa **Resolução**, selecione a resolução desejada para a tela selecionada.

As resoluções compatíveis serão listadas [na seção de requisitos de hardware e software](#).

Se o valor **Máxima possível** for selecionado, o valor mais alto do parâmetro compatível com o monitor e com o Kaspersky Thin Client será definido.

- Na lista suspensa **Orientação**, selecione a posição da tela:
 - **Paisagem**: a posição padrão da tela.
 - **Paisagem invertida**: a tela gira 180°.
 - **Retrato**: a tela gira 90°.
 - **Retrato invertido**: a tela gira 270°.

Conforme cada configuração vai sendo alterada, uma janela de contagem regressiva será exibida.

6. Na janela exibida, confirme as alterações clicando em **Salvar**. Caso queira descartar as alterações e continuar personalizando as configurações, clique em **Cancelar**.

As alterações serão salvas.

Definição das configurações de economia de energia

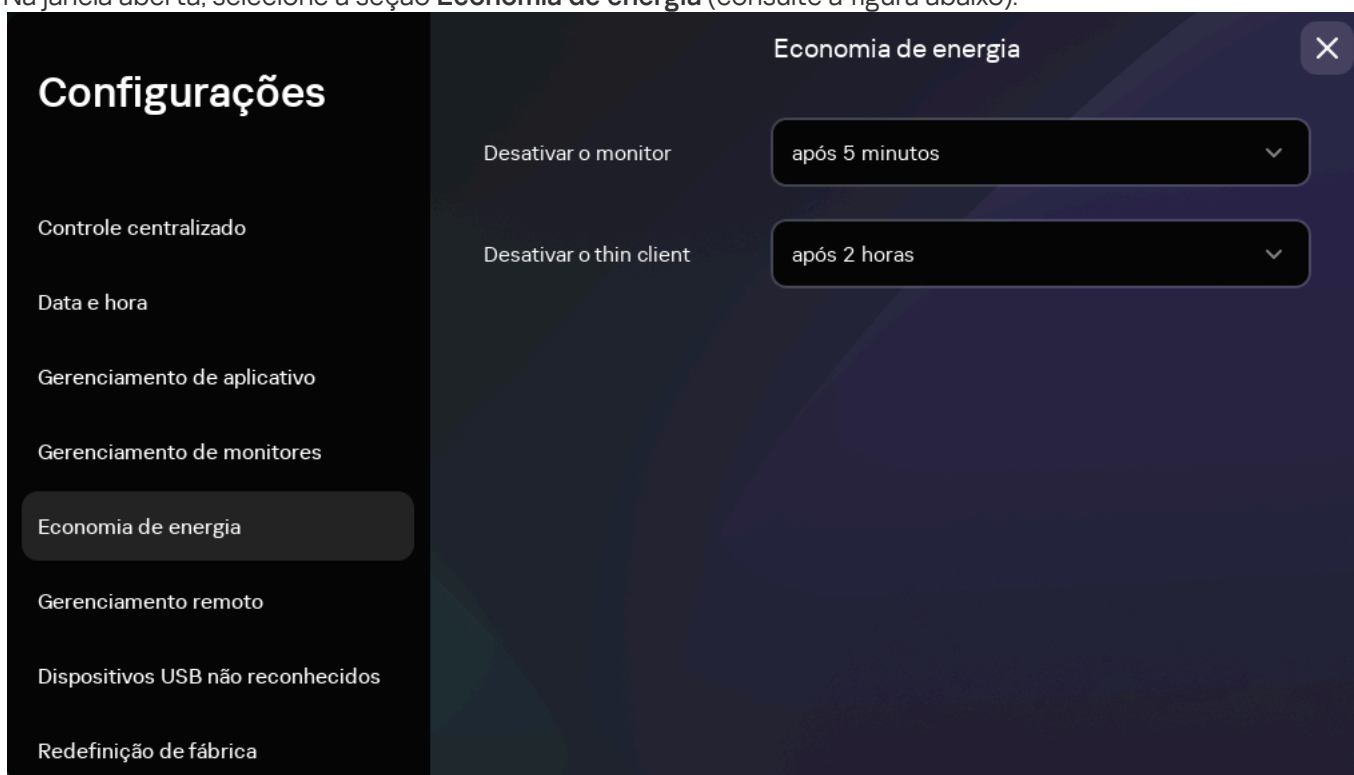
Se o thin client estiver incluído em um [grupo de administração @](#), os valores das configurações especificadas neste artigo poderão ser aplicados pelo Web Console. Se for esse o caso, não será possível definir essas configurações na interface do Kaspersky Thin Client.

As configurações especificadas neste artigo podem estar [ocultas no Kaspersky Thin Client](#).

É possível configurar um período de tempo limite ocioso para desativar o monitor. O monitor será ativado automaticamente ao clicar no mouse, pressionar uma tecla do teclado ou mover o cursor do mouse. Também é possível configurar um período de inatividade do Kaspersky Thin Client após o qual o thin client será desativado. Para retomar as operações do thin client, será preciso ativá-lo.

Para definir as configurações de economia de energia:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Economia de energia** (consulte a figura abaixo).



Configurações. Seção Economia de energia

3. Na lista suspensa **Desativar o monitor**, selecione o período de inatividade do sistema após o qual o monitor será desativado.
4. Na lista suspensa **Desativar o thin client**, selecione o período de inatividade do sistema após o qual o thin client será desativado.

Também é possível definir as configurações de economia de energia por meio do Kaspersky Security Center Web Console.

Definição de configurações de gerenciamento remoto de thin clients na interface do Kaspersky Thin Client

Se o thin client estiver incluído em um [grupo de administração](#), os valores das configurações especificadas neste artigo poderão ser aplicados pelo Web Console. Se for esse o caso, não será possível definir essas configurações na interface do Kaspersky Thin Client.

As configurações especificadas neste artigo podem estar [ocultas no Kaspersky Thin Client](#).

Na interface do Kaspersky Thin Client, é possível definir as seguintes configurações de [gerenciamento remoto](#):

- Modo de acesso de gerenciamento remoto.

Define as condições e o procedimento para conexão com um thin client.

- O modo de acesso à sessão remota em execução no thin client quando a conexão é estabelecida (doravante também chamado de "tela do ambiente remoto").

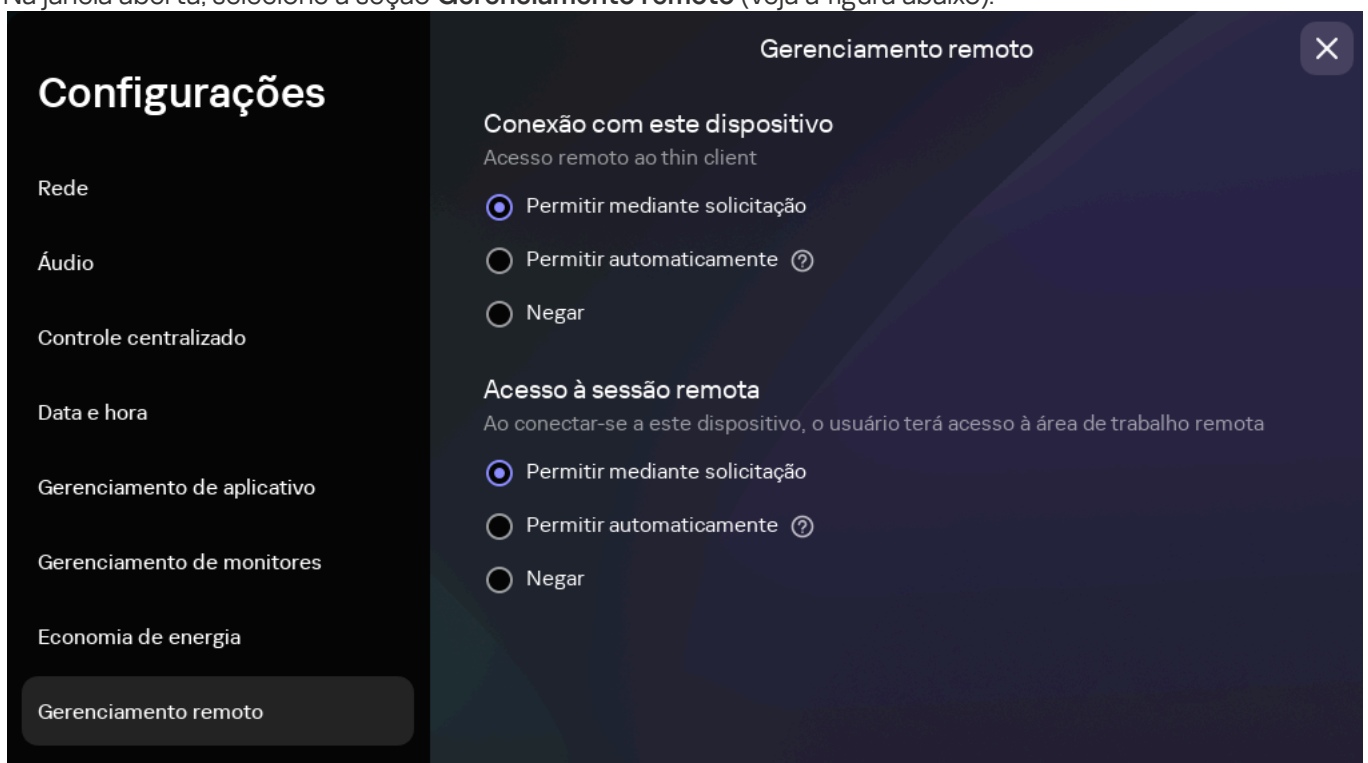
Pode ser necessário restringir o acesso à tela do ambiente remoto se o usuário do thin client estiver trabalhando com dados sensíveis ou confidenciais.

Para definir as configurações de gerenciamento remoto de um thin client:

1. [Ative o thin client](#).

2. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.

3. Na janela aberta, selecione a seção **Gerenciamento remoto** (veja a figura abaixo).



Configurações. Seção Gerenciamento remoto

4. No grupo de configurações **Conexão com este dispositivo**, selecione o modo de acesso para gerenciamento remoto do thin client:

- **Permitir automaticamente**

Nesse modo, o administrador poderá se conectar remotamente ao thin client após o usuário [aceitar a solicitação de gerenciamento remoto na interface do Kaspersky Thin Client](#). Caso o usuário rejeite a solicitação, a conexão será encerrada. Caso não haja resposta em 30 segundos, a conexão será estabelecida automaticamente.

Para garantir a segurança do dispositivo, use esse modo somente se o thin client estiver conectado com o Kaspersky Security Center.

- **Permitir mediante solicitação**

Nesse modo, o administrador poderá se conectar remotamente ao thin client somente após o usuário [aceitar a solicitação de gerenciamento remoto na interface do Kaspersky Thin Client](#). Caso o usuário rejeite a solicitação, a conexão será encerrada.

- **Negar**

Nesse modo, o administrador não pode se conectar remotamente ao thin client.

Ao definir o modo **Permitir automaticamente** ou **Permitir mediante solicitação**, o grupo de configurações **Acesso à sessão remota** é exibido.

5. No grupo de configurações **Acesso à sessão remota**, selecione o modo de acesso à tela do ambiente remoto:

- **Permitir automaticamente**

Nesse modo, após se conectar ao thin client, o administrador pode acessar a tela do ambiente remoto sem confirmação do usuário.

- **Permitir mediante solicitação**

Nesse modo, após se conectar ao thin client, o administrador pode acessar a tela do ambiente remoto somente após o usuário [confirmar a solicitação de acesso na interface do Kaspersky Thin Client](#).

- **Negar**

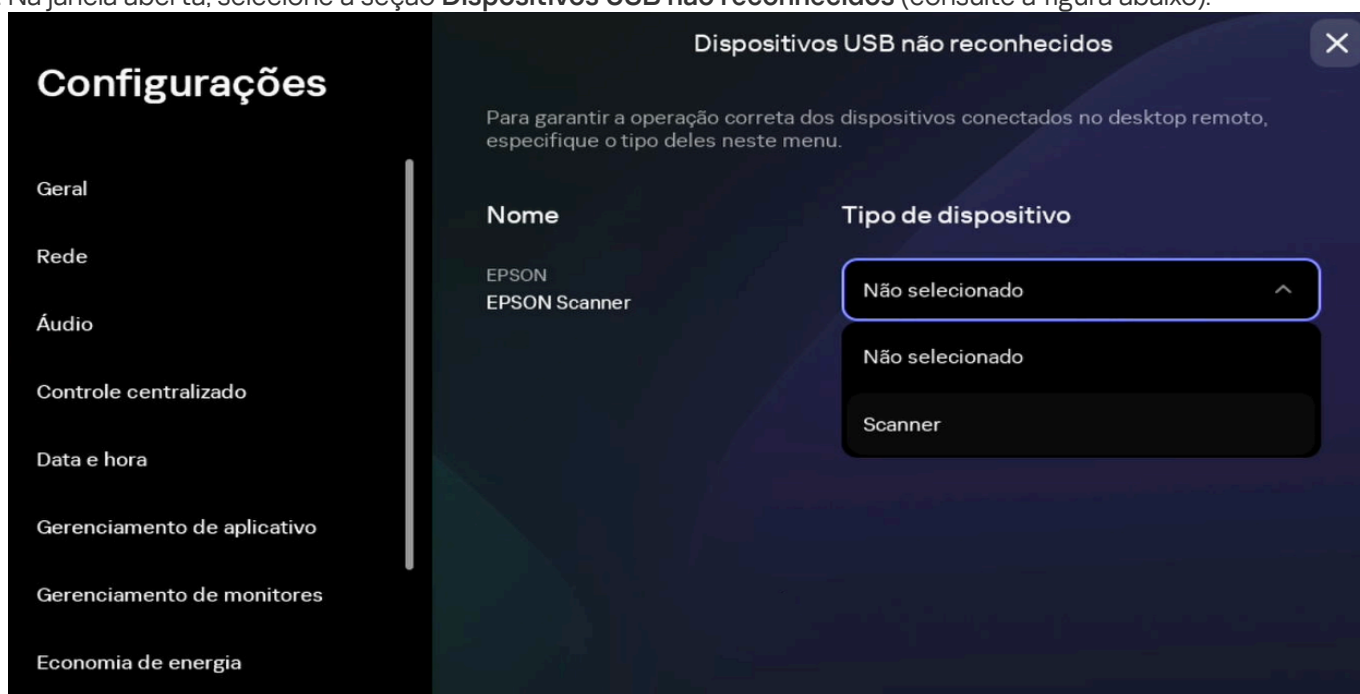
Nesse modo, o administrador não pode gerenciar remotamente o thin client até que o usuário [encerre a sessão remota](#) manualmente.

Alteração do tipo de dispositivos USB não reconhecidos

Por padrão, o Kaspersky Thin Client detecta automaticamente o tipo de [dispositivo USB compatível](#) conectado ao thin client. Caso o sistema não consiga determinar o tipo do dispositivo conectado (aqui também referido como um "dispositivo não reconhecido"), é necessário selecionar manualmente o tipo na interface do Kaspersky Thin Client para garantir a operação correta.

Para alterar manualmente o tipo de um dispositivo USB não reconhecido:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Dispositivos USB não reconhecidos** (consulte a figura abaixo).



Configurações. Seção Dispositivos USB não reconhecidos

Será possível visualizar uma lista de dispositivos USB cujos tipos não puderam ser identificados pelo sistema. O nome do modelo e o fabricante são exibidos para cada dispositivo caso o sistema tenha conseguido obter essas informações.

Caso nenhum dispositivo não reconhecido seja detectado, a lista estará vazia.

3. Na lista suspensa ao lado do nome do dispositivo pertinente, selecione seu tipo.

Na versão atual do Kaspersky Thin Client, somente o seguinte tipo de dispositivo USB está disponível: scanner.

O tipo de dispositivo não reconhecido será alterado e salvo no sistema. Agora, é possível [redirecionar o dispositivo para um ambiente remoto](#).

Redefinição das configurações do Kaspersky Thin Client

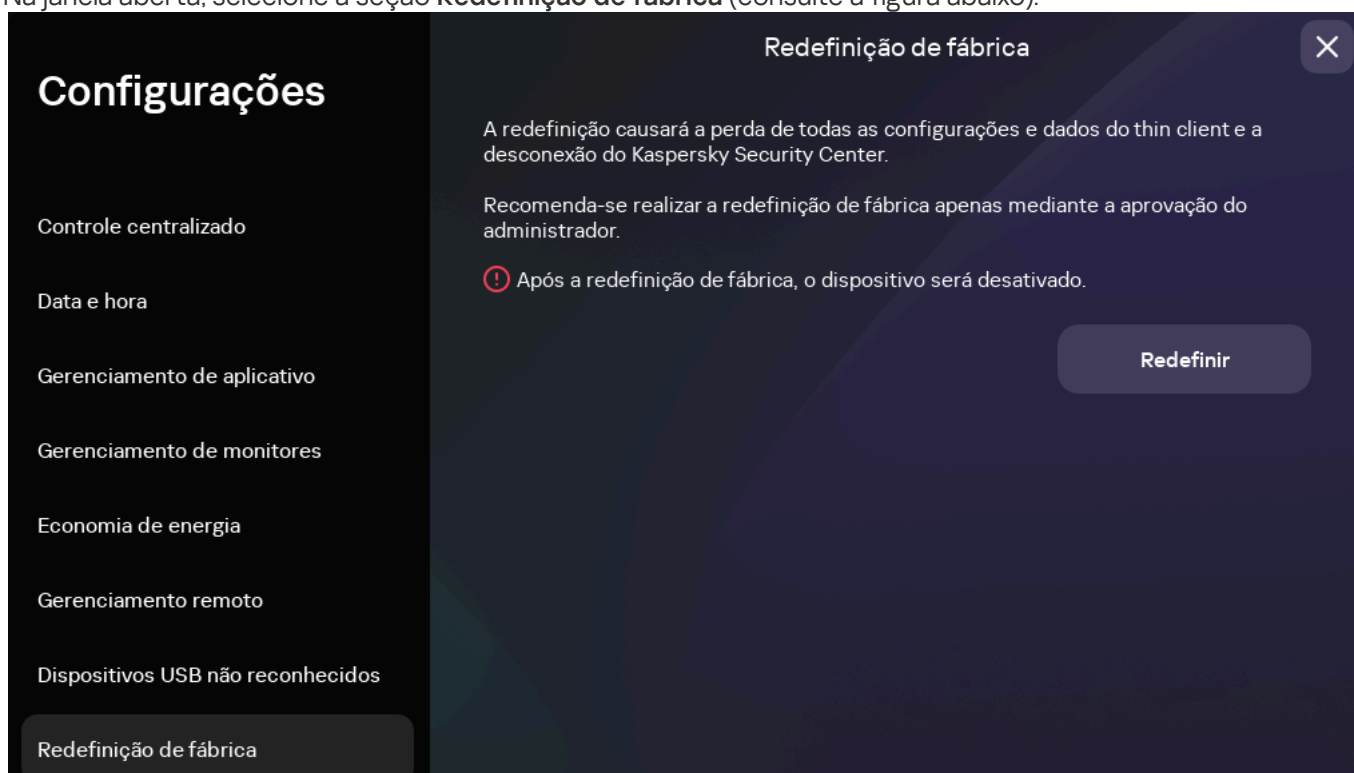
A redefinição resultará na perda de todas as configurações definidas e de todos os dados do Kaspersky Thin Client (exceto o [log de auditoria](#) e a data do sistema) e desconectará o dispositivo do Kaspersky Security Center. Recomendamos executar a redefinição somente após a aprovação do administrador de sua empresa.

Se o thin client estiver incluído em um [grupo de administração](#), os valores das configurações especificadas neste artigo poderão ser aplicados pelo Web Console. Se for esse o caso, não será possível definir essas configurações na interface do Kaspersky Thin Client.

As configurações especificadas neste artigo podem estar [ocultas no Kaspersky Thin Client](#).

Para redefinir as configurações do Kaspersky Thin Client:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Redefinição de fábrica** (consulte a figura abaixo).



Configurações. Seção Redefinição de fábrica

Então, todas as configurações definidas do Kaspersky Thin Client serão restauradas para seus valores originais (padrão), todos os dados no dispositivo serão excluídos (exceto o [log de auditoria](#) e a data do sistema) e o Kaspersky Thin Client será desconectado do Kaspersky Security Center. Após a redefinição, o thin client será desativado.

Para executar uma redefinição de fábrica de um thin client incluído em um grupo de administração:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Configurações** no menu aberto.
2. Na janela aberta, selecione a seção **Redefinição de fábrica**.
3. Na janela aberta, clique no botão **Redefinir**.

A janela **Confirmar redefinição** será exibindo um código de confirmação.

4. Forneça o código de confirmação ao administrador do Kaspersky Security Center. Os detalhes de contato do administrador são fornecidos na janela **Confirmar redefinição**. O administrador do Kaspersky Security Center envia um código de confirmação para você como resposta.
5. Clique em **Avançar**.
6. Na janela aberta **Código de confirmação**, insira o código fornecido pelo administrador do Kaspersky Security Center e clique no botão **Confirmar**.

Então, todas as configurações definidas do Kaspersky Thin Client serão restauradas para seus valores originais (padrão), todos os dados no dispositivo serão excluídos (exceto o [log de auditoria](#) e a data do sistema) e o Kaspersky Thin Client será desconectado do Kaspersky Security Center. Após a redefinição, o thin client será desativado.

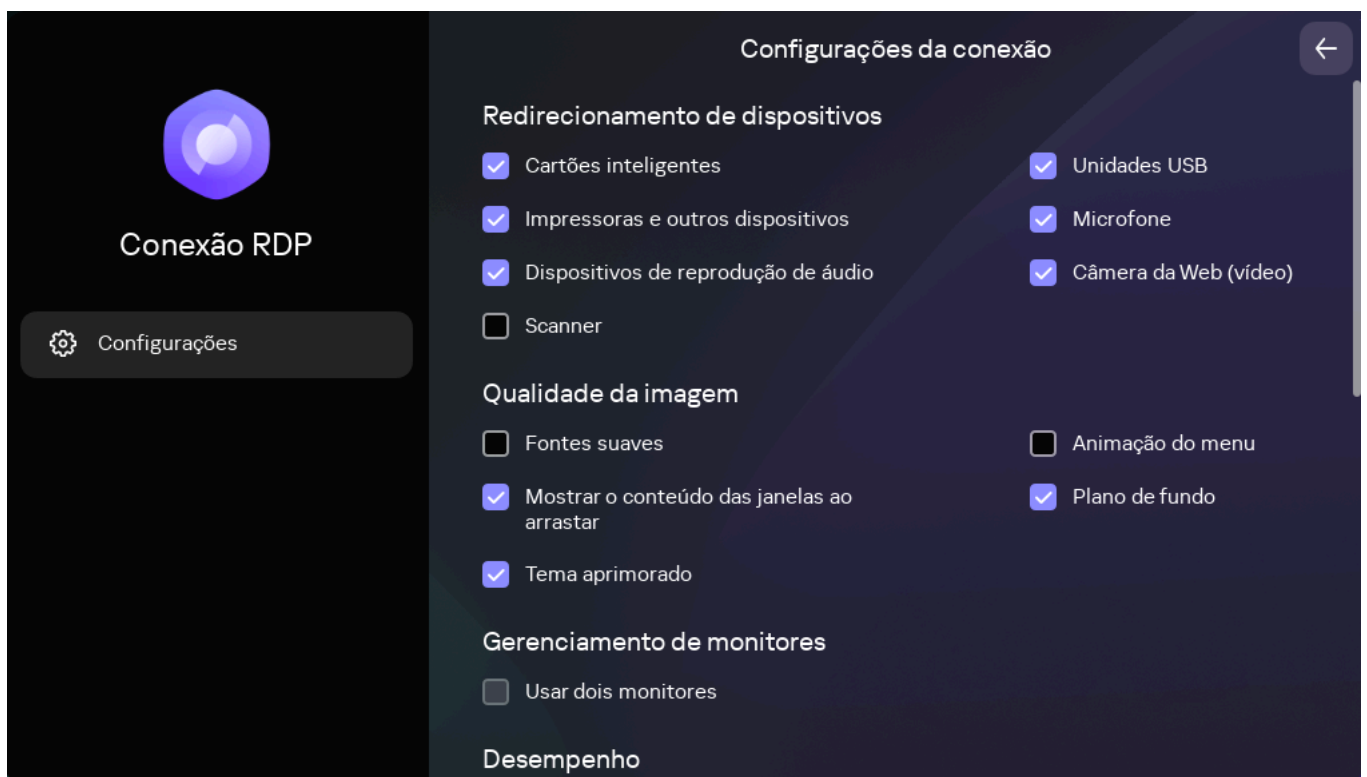
Definição das configurações de conexão com um ambiente remoto pelo aplicativo RDP

No aplicativo RDP, é possível definir as configurações para se [conectar a um aplicativo virtual ou um desktop remoto](#) via RDP, inclusive por meio de uma conexão automática com um ambiente remoto.

Para definir as configurações para conexão com um ambiente remoto no aplicativo RDP:

1. No desktop do Kaspersky Thin Client, clique no botão **RDP**.
2. Na parte esquerda da janela de conexão que se abre, clique em **Configurações**.

Isso abre uma janela na qual é possível definir as configurações para conexão com um ambiente remoto (veja a figura abaixo).



Janela para configurar uma conexão com um ambiente remoto no aplicativo RDP

3. No bloco de configurações **Redirecionamento de dispositivos**, selecione os dispositivos a serem redirecionados para o ambiente remoto: **Cartões inteligentes**, **Unidades USB**, **Impressoras e outros dispositivos**, **Microfone**, **Dispositivos de reprodução de áudio**, **Câmera da Web (vídeo)** e **Scanner**.

O volume do áudio e outras configurações são gerenciados no ambiente remoto.

Para redirecionar corretamente os dispositivos USB para um desktop remoto usando o sistema operacional Windows 10, é preciso ativar o Microsoft Remote Desktop Services e permitir o redirecionamento de dispositivos Plug and Play nas configurações do Remote Desktop Services. Para o Microsoft Windows Server 2016 e 2019, é necessário ativar as conexões remotas por meio dos Serviços de Desktop Remoto e permitir a configuração das regras de gerenciamento remoto nesses serviços.

4. No bloco **Qualidade da imagem**, marque as caixas de seleção ao lado das configurações gráficas do desktop remoto que deseja usar: **Fontes suaves**, **Animação do menu**, **Plano de fundo**, **Mostrar o conteúdo das janelas ao arrastar** e **Tema aprimorado**.

Ativar as configurações de exibição do desktop remoto remota poderá afetar a velocidade das operações do Kaspersky Thin Client.

5. Caso dois monitores estejam instalados em sua estação de trabalho e o usuário quiser que uma imagem do desktop remoto seja exibida em ambos os monitores, marque a caixa de seleção **Usar dois monitores** no bloco **Gerenciamento de monitores**.
6. Para melhorar o desempenho quando conectado com desktops remotos ou aplicativos, no bloco **Desempenho**, marque **Melhorar o desempenho gráfico**.
7. Para [se conectar a um desktop remoto ou aplicativo virtual](#) automaticamente quando o aplicativo RDP for iniciado, no bloco **Conexão automática**, marque a caixa de seleção **Conectar automaticamente**.
- Para ativar a função, é necessário se conectar e desconectar manualmente do ambiente remoto uma vez. Ao fazer isso, os seguintes dados para a conexão com o servidor RDP serão salvos no armazenamento do thin client: nome de usuário, endereço do servidor e senha. Na próxima vez que o aplicativo RDP for iniciado, essas credenciais serão usadas para iniciar automaticamente uma conexão ao ambiente remoto. Caso a função de conexão automática seja desativada, a senha salva será excluída do armazenamento do dispositivo.
- Para se conectar automaticamente ao ambiente remoto no aplicativo RDP imediatamente após a inicialização do Kaspersky Thin Client, [configure a inicialização automática do aplicativo](#) na seção **Configurações**.
8. Caso precise usar o Microsoft Remote Desktop Connection Broker para conexão com um desktop remoto, use o campo **ID da coleta do Remote Desktop Connection Broker** para especificar o ID da coleção no formato `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` refere-se ao identificador específico da coleção).
- Caso precise iniciar um aplicativo virtual, especifique o apelido do aplicativo no campo **Apelido do aplicativo**.
9. Caso queira restaurar automaticamente uma conexão do desktop remoto que foi desconectada inesperadamente, marque a caixa de seleção **Conectar novamente se a conexão for perdida**.
10. Clique na seta voltar no canto superior direito da janela para retornar à janela de conexão.

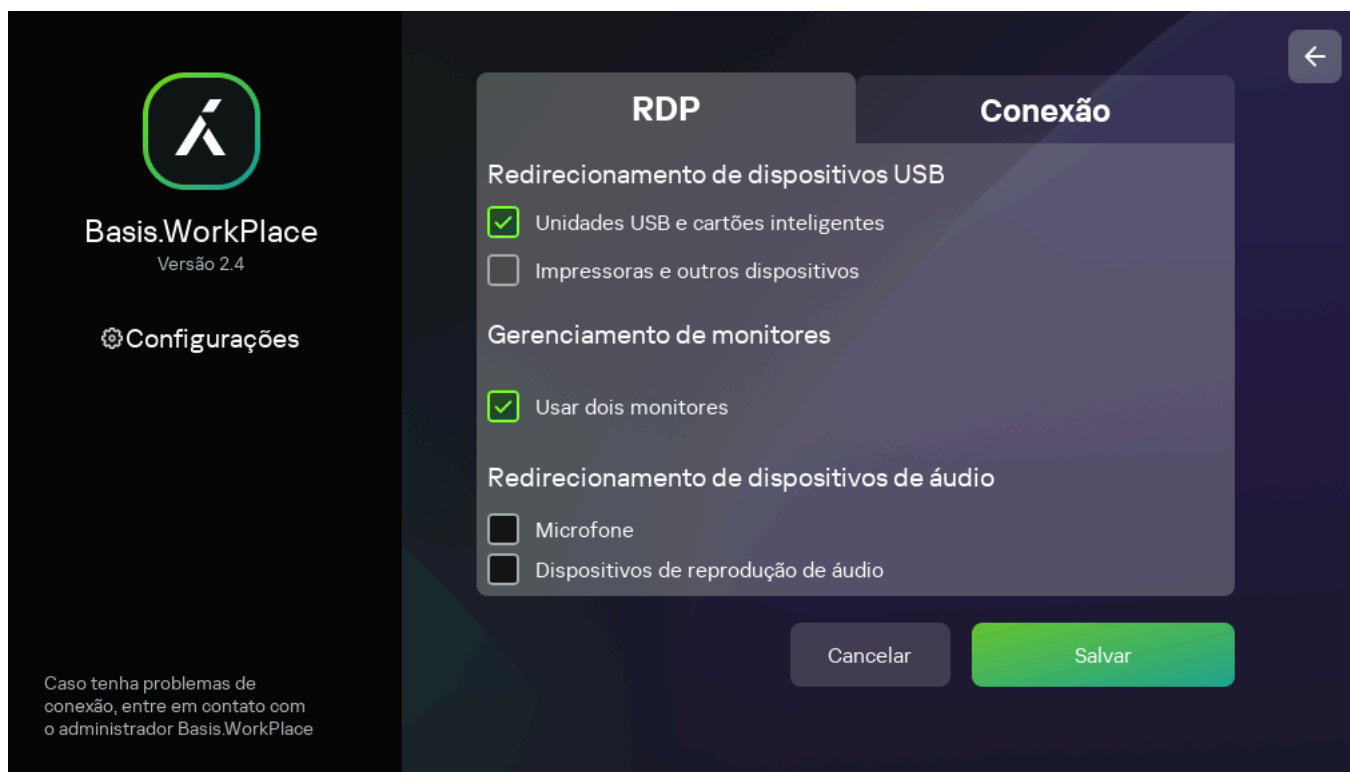
Definição das configurações de conexão com um ambiente remoto pelo aplicativo Basis.WorkPlace

Por meio do aplicativo Basis.WorkPlace, é possível definir as configurações para a conexão com um ambiente remoto implementado na infraestrutura do aplicativo.

Para definir as configurações para conexão com um ambiente remoto no aplicativo Basis.WorkPlace:

1. No desktop do Kaspersky Thin Client, clique no botão **Basis.WorkPlace**.
2. Na janela de conexão aberta do desktop remoto, clique em **Configurações** na parte esquerda.

Isso abre uma janela na qual é possível definir as configurações para redirecionar dispositivos para um ambiente remoto (veja a figura abaixo).



Janela para configurar o redirecionamento de dispositivos para um ambiente remoto implementado em uma infraestrutura Basis.WorkPlace

3. Para definir as configurações de redirecionamento de dispositivos para um ambiente remoto:

- No bloco de configurações **Redirecionamento de dispositivos USB**, selecione os dispositivos a serem redirecionados para o ambiente remoto: **Unidades USB e cartões inteligentes**, **Impressoras e outros dispositivos**.
- Caso dois monitores estejam instalados em sua estação de trabalho e o usuário quiser que uma imagem do desktop remoto seja exibida em ambos os monitores, marque a caixa de seleção **Usar dois monitores** no bloco **Gerenciamento de monitores**.
- No bloco de configurações **Redirecionamento de dispositivos de áudio**, selecione os dispositivos a serem redirecionados para o ambiente remoto: **Dispositivos de reprodução de áudio** e **Microfone**.
- O volume do áudio e outras configurações são gerenciados no ambiente remoto.

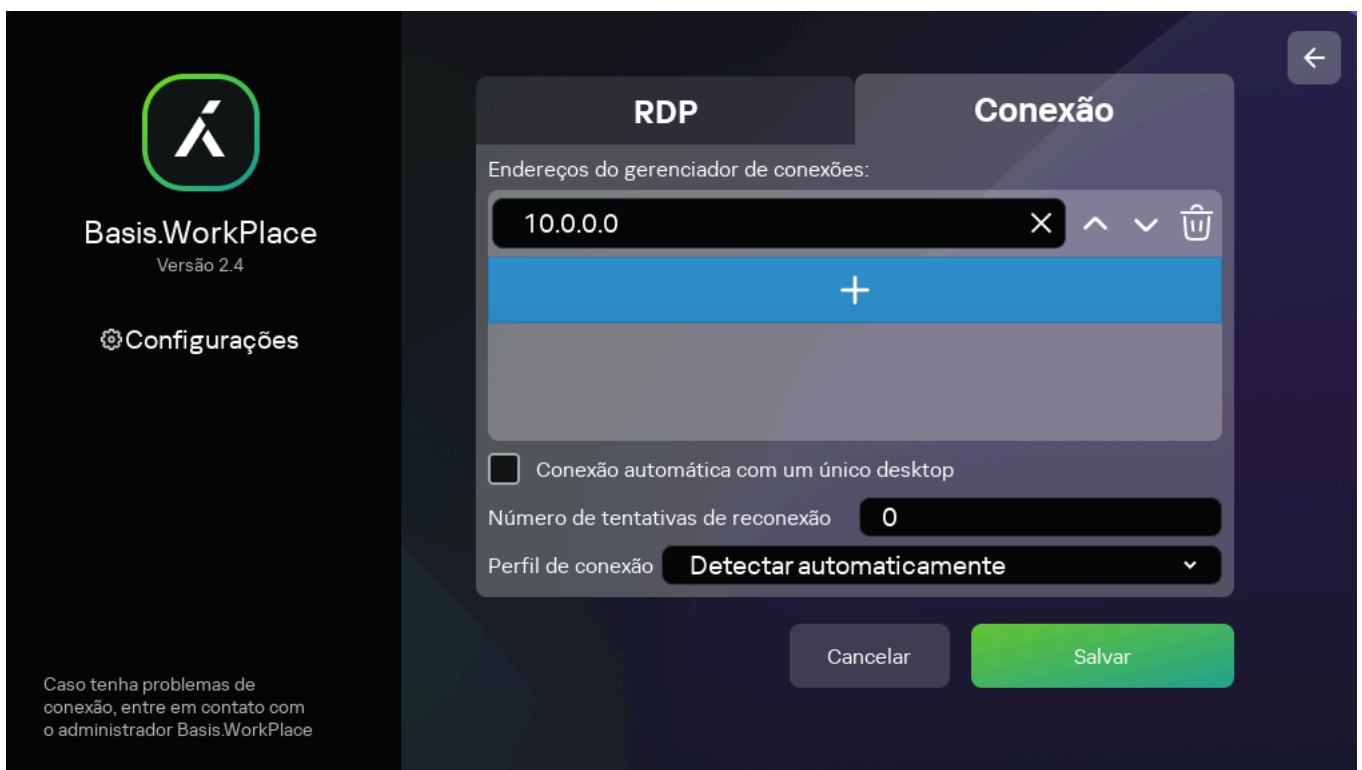
O redirecionamento de dispositivos USB para um desktop remoto gerenciado pelo Basis.WorkPlace pode ser bloqueado pelo administrador do Basis.WorkPlace.

4. Para definir as configurações da conexão com um ambiente remoto geograficamente distribuído, vá para a guia **Conexão** (veja a figura abaixo).

Para obter uma descrição detalhada das configurações desta guia, consulte o [Guia de Instalação Geodistribuída](#) no site Basis.WorkPlace.

Faça o seguinte na guia selecionada:

- a. Na seção **Endereços do gerenciador de conexões**, clique em + e especifique o endereço IP do [broker](#) Basis.WorkPlace no campo exibido. É possível adicionar no máximo quatro endereços IP.
- b. No campo **Número de tentativas de reconexão**, insira o número de vezes que o Kaspersky Thin Client deve tentar se reconectar com o broker Basis.WorkPlace, caso seja desconectado. É possível indicar no máximo cinco tentativas de reconexão.
- c. Na lista suspensa **Perfil de conexão**, selecione o tipo de conexão entre o Kaspersky Thin Client e o broker Basis.WorkPlace. O tipo de conexão depende da velocidade da conexão. Os seguintes valores estão disponíveis:
 - Detectar automaticamente
 - Modem
 - Conexão de banda larga de baixa velocidade
 - Satélite
 - Conexão de banda larga de alta velocidade
 - Rede de longa distância
 - Rede de área local



Janela para configurar uma conexão com um ambiente remoto distribuído geograficamente e implementado em uma infraestrutura Basis.WorkPlace

5. Clique em **Salvar** na parte inferior da janela para salvar as alterações.
6. Clique na seta voltar no canto superior direito da janela para retornar à janela de conexão com ambiente remoto.

Gerenciamento do acesso às configurações do Kaspersky Thin Client

É possível configurar a interface do Kaspersky Thin Client para exibir ou ocultar as configurações que são definidas somente uma vez e não são mais usadas nos principais cenários de operação do thin client.

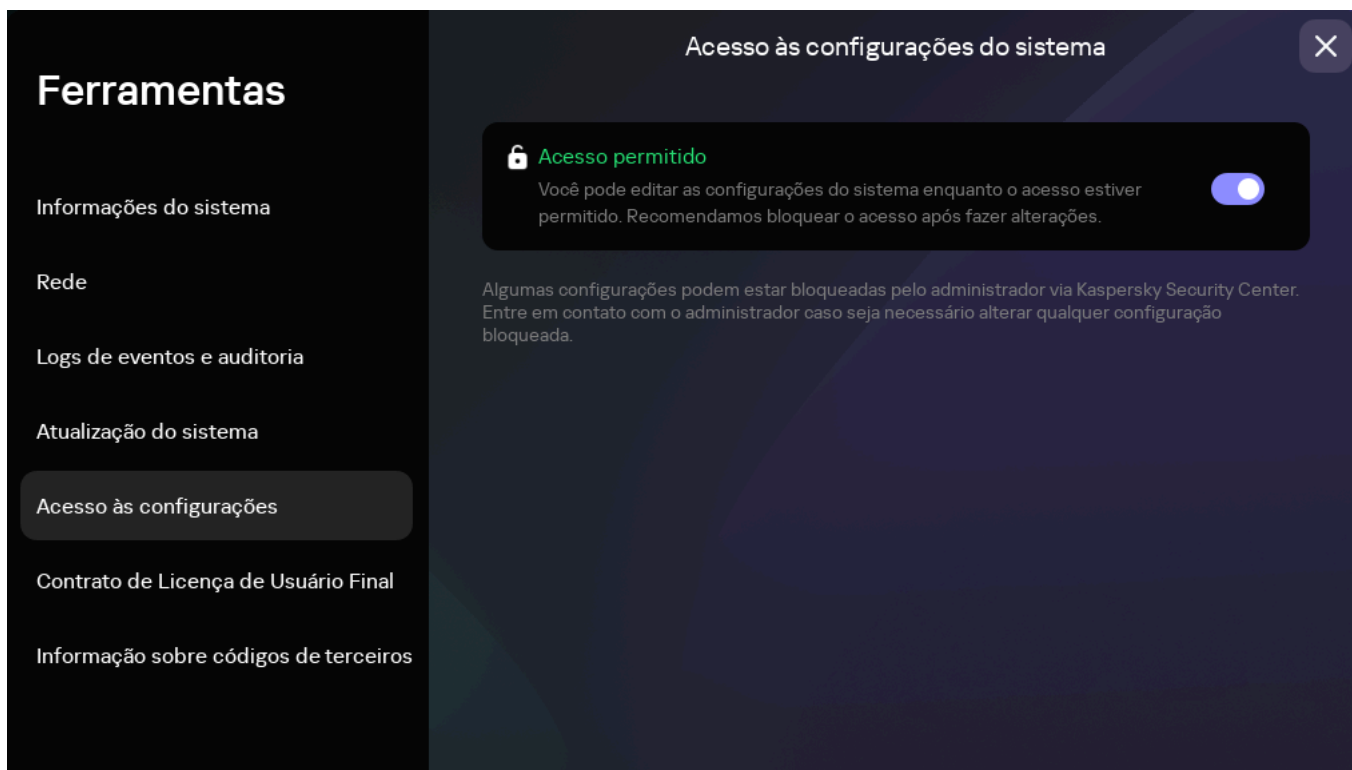
Caso o thin client esteja incluído em um [grupo de administração](#), os valores das configurações poderão ser aplicados por meio do Web Console. A edição dessas configurações aplicadas será bloqueada na interface do Kaspersky Thin Client e você não poderá ativar ou desativar sua exibição.

Para ativar ou desativar a exibição das configurações do Kaspersky Thin Client:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Ferramentas** no menu aberto.
2. Na janela aberta, selecione a seção **Acesso às configurações** (consulte a figura abaixo) e execute uma das seguintes ações:
 - Caso precise ocultar as configurações, mova o botão de alternância para a posição **Acesso bloqueado**. Todas as seguintes configurações ficarão ocultas na interface do thin client:
 - [Configurações de conexão RDP](#)
 - [Configurações de conexão do Basis.WorkPlace](#)
 - [Configurações gerais](#)
 - [Configurações de rede](#)
 - [Configurações de conexão do Kaspersky Security Center](#)
 - [Data e hora](#)
 - [Configurações de economia de energia](#)
 - [Layout de monitores](#)
 - [Redefinição das configurações do Kaspersky Thin Client](#)

- Caso seja necessário exibir as configurações, mova o botão de alternância para a posição **Acesso permitido**.

As configurações serão exibidas. Será possível definir novos valores para essas configurações.



Ferramentas. Seção Acesso às configurações

Gerenciamento do Kaspersky Thin Client instalado em um thin client

Esta seção descreve o principal cenário de operação do Kaspersky Thin Client e contém instruções de uso para o Kaspersky Thin Client.

Cenário: funcionamento do Kaspersky Thin Client em um thin client

O cenário principal para trabalhar no Kaspersky Thin Client instalado em um [thin client](#) consiste nos seguintes estágios:

1 Preparação do Kaspersky Thin Client para inicialização

Conecte os [periféricos](#) com o thin client antes de iniciá-lo pela primeira vez.

2 Inicialização do Kaspersky Thin Client

[Ative](#) o thin client para começar.

3 Início de uma sessão remota

[Conecte-se a um ambiente remoto](#) e comece a trabalhar em uma sessão remota.

4 Bloqueio e desbloqueio de sessão remota

[Bloqueie sua sessão remota](#) se precisar se afastar de sua estação de trabalho por algum tempo. Retome suas atividades ao retornar.

5 Encerramento de uma conexão remota

[Encerre sua sessão remota](#) ao finalizar suas atividades.

6 Desativação do Kaspersky Thin Client

Desative o thin client no final do dia de trabalho.

Conexão com um ambiente remoto

Esta seção fornece informações sobre como se conectar a um [ambiente remoto](#) por meio dos aplicativos do Kaspersky Thin Client e como começar a trabalhar em uma [sessão remota](#).

As seguintes limitações se aplicam durante a conexão a um ambiente remoto no Kaspersky Thin Client:

- A troca de arquivos entre o Kaspersky Thin Client e o ambiente remoto não é compatível.
- O compartilhamento entre o Kaspersky Thin Client e o ambiente remoto não é compatível.
- Não há suporte para iniciar várias sessões remotas simultaneamente ou estabelecer conexão com vários ambientes remotos simultaneamente em uma única sessão remota.

O Kaspersky Thin Client utiliza criptografia [TLS](#) (versões 1.2 e 1.3) para proteger todas as sessões remotas e evitar que os dados sejam interceptados ou falsificados.

Para se conectar a ambientes remotos que executam o Microsoft Windows, o Kaspersky Thin Client é compatível com os seguintes pacotes de codificação:

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

Conexão com um ambiente remoto pelo aplicativo RDP

No aplicativo RDP, é possível se conectar a [desktops remotos](#) e [aplicativos virtuais](#) via RDP.

Conexão com um desktop remoto

Para se conectar a um desktop remoto no aplicativo RDP:

1. [Ativar o Kaspersky Thin Client](#).
2. No desktop do Kaspersky Thin Client, clique no botão **RDP**.
3. Na janela de conexão aberta, especifique as configurações de conexão:
 - a. No campo **Servidor**, especifique o endereço IP ou o nome do servidor Microsoft Remote Desktop Connection Broker.

O Kaspersky Thin Client salva o último endereço inserido do servidor com o qual uma conexão foi estabelecida com sucesso para que não seja necessário inseri-lo novamente ao reconectar.

b. No campo **Nome de usuário**, insira o nome de usuário local ou do domínio. É possível especificar o nome de usuário do domínio no formato **Domínio\Nome de usuário** ou no formato **Nome de usuário**.

O Kaspersky Thin Client salva o nome de usuário inserido pela última vez e que se conectou com sucesso com o servidor para que não seja necessário inseri-lo novamente ao reconectar.

c. No campo **Senha**, insira a senha do usuário.

Caso não tenha [ativado a função de conexão automática](#), a senha não será salva, e ela deverá ser inserida novamente na próxima conexão.

4. Para [definir as configurações](#) de conexão com um desktop remoto, clique em **Configurações** na parte esquerda da janela.

5. Pressione **Enter** ou clique em **Conectar**.

Você verá uma janela solicitando que adicione um certificado para se conectar ao ambiente remoto se as condições a seguir forem atendidas:

- Você está se conectando a um ambiente remoto na interface do Kaspersky Thin Client pela primeira vez.
- O thin client está em um dos seguintes estados:
 - não conectado ao Kaspersky Security Center
 - não adicionado ao [grupo de administração](#) 
 - [nenhum certificado para conexão ao ambiente remoto foi adicionado](#) para o grupo de administração ao qual o thin client pertence

Verifique as configurações do certificado e clique no botão **Adicionar certificado**. O certificado será adicionado ao armazenamento de certificados do sistema do Kaspersky Thin Client e será usado para conexões subsequentes.

6. Caso o ID da coleta do Remote Desktop Connection Broker tenha sido especificado ao [configurar uma conexão do desktop remoto](#) e vários desktops estiverem disponíveis, na janela aberta de seleção do desktop remoto, clique no botão com o nome do desktop com o qual deseja se conectar.

Uma janela de desktop remoto é aberta e uma sessão remota é iniciada.

Conexão com um aplicativo virtual

Para se conectar a um [aplicativo virtual](#)  no aplicativo RDP:

1. [Ativar o Kaspersky Thin Client](#).

2. No desktop do Kaspersky Thin Client, clique no botão **RDP**.

3. Na janela de conexão aberta, especifique as configurações de conexão:

a. No campo **Servidor**, especifique o endereço IP ou o nome do servidor Microsoft Remote Desktop Connection Broker.

O Kaspersky Thin Client salva o último endereço inserido do servidor com o qual uma conexão foi estabelecida com sucesso para que não seja necessário inseri-lo novamente ao reconectar.

b. No campo **Nome de usuário**, insira o nome de usuário local ou do domínio. É possível especificar o nome de usuário do domínio no formato `Domínio\Nome de usuário` ou no formato `Nome de usuário`.

O Kaspersky Thin Client salva o nome de usuário inserido pela última vez e que se conectou com sucesso com o servidor para que não seja necessário inseri-lo novamente ao reconectar.

c. No campo **Senha**, insira a senha do usuário.

Caso não tenha [ativado a função de conexão automática](#), a senha não será salva, e ela deverá ser inserida novamente na próxima conexão.

4. Clique em **Configurações** na parte esquerda da janela.

5. No campo **ID da coleta do Remote Desktop Connection Broker**, especifique o ID da coleção no formato `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` refere-se ao identificador específico da coleção).

6. No campo **Apelido do aplicativo**, especifique o apelido do aplicativo virtual que deseja abrir.

O Kaspersky Thin Client salva o apelido inserido pela última vez para que não seja necessário inseri-lo novamente ao reconectar.

7. Clique na seta voltar no canto superior direito da janela para retornar à janela de conexão.

8. Na janela de conexão, pressione **Enter** ou clique em **Conectar**.

Você verá uma janela solicitando que adicione um certificado para se conectar ao ambiente remoto se as condições a seguir forem atendidas:

- Você está se conectando a um ambiente remoto na interface do Kaspersky Thin Client pela primeira vez.
- O thin client está em um dos seguintes estados:
 - não conectado ao Kaspersky Security Center
 - não adicionado ao [grupo de administração](#) 
 - [nenhum certificado para conexão ao ambiente remoto foi adicionado](#) para o grupo de administração ao qual o thin client pertence

Verifique as configurações do certificado e clique no botão **Adicionar certificado**. O certificado será adicionado ao armazenamento de certificados do sistema do Kaspersky Thin Client e será usado para conexões subsequentes.

Uma janela de aplicativo virtual é aberta e uma sessão remota é iniciada.

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

passa o mouse sobre o ícone do aplicativo no [painel de conexão](#) na parte superior da tela e selecione a janela pertinente na lista suspensa.

Conexão com um ambiente remoto pelo aplicativo Basis.WorkPlace

No aplicativo Basis.WorkPlace, é possível se conectar a desktops virtuais Basis.WorkPlace.

Os usuários não podem iniciar uma alteração de senha no Kaspersky Thin Client.

Para se conectar a um desktop virtual no aplicativo Basis.WorkPlace:

1. [Ativar o Kaspersky Thin Client](#).

2. No desktop do Kaspersky Thin Client, clique no botão **Basis.WorkPlace**.

3. Na janela de conexão aberta, especifique as configurações de conexão do Basis.WorkPlace:

- a. No campo **Servidor**, especifique o endereço IP ou o nome do servidor [broker](#)  Basis.WorkPlace.

O Kaspersky Thin Client salva o endereço do broker Basis.WorkPlace com o qual uma conexão foi estabelecida com sucesso para que não seja necessário inseri-lo novamente ao reconectar.

- b. No campo **Domínio**, insira o nome do domínio.

- c. No campo **Nome de usuário**, insira o nome de usuário.

O Kaspersky Thin Client salva o nome de usuário que se conectou pela última vez com sucesso ao Basis.WorkPlace para que não seja necessário inseri-lo novamente ao reconectar.

- d. No campo **Senha**, insira a senha do usuário.

A senha do usuário não é salva; na próxima vez que você se conectar, será necessário inserir a senha novamente.

Caso o número permitido de tentativas de entrada de senha incorreta seja excedido, a conta do usuário será bloqueada. A mensagem correspondente será exibida na janela de conexão do desktop virtual. O número permitido de tentativas de entrada de senha é definido pela política de segurança ativa definida pelo administrador do Basis.WorkPlace.

4. Pressione **Enter** ou clique em **Conectar**.

Você verá uma janela solicitando que adicione um certificado para se conectar ao ambiente remoto se as condições a seguir forem atendidas:

- Você está se conectando a um ambiente remoto na interface do Kaspersky Thin Client pela primeira vez.
- O thin client está em um dos seguintes estados:
 - não conectado ao Kaspersky Security Center
 - não adicionado ao [grupo de administração](#) 
 - [nenhum certificado para conexão ao ambiente remoto foi adicionado](#) para o grupo de administração ao qual o thin client pertence

Verifique as configurações do certificado e clique no botão **Adicionar certificado**. O certificado será adicionado ao armazenamento de certificados do sistema do Kaspersky Thin Client e será usado para conexões subsequentes.

Uma janela de infraestrutura do Basis.WorkPlace será aberta com os desktops virtuais disponíveis.

5. Caso seja necessário atualizar a lista de desktops virtuais, clique no botão **Recarregar**.

6. Clique no botão com o nome do desktop virtual ao qual deseja se conectar.

Uma janela do desktop virtual será exibida. Uma sessão remota será iniciada.

O acesso ao Basis.WorkPlace pode ser restringido pelo administrador. Por exemplo, o administrador pode bloquear a conta de usuário ou impedir o acesso a desktops virtuais que anteriormente estavam acessíveis à conta de usuário. Caso haja problemas ao se conectar ao ambiente remoto, entre em contato com o administrador de sua organização.

Conexão com um ambiente remoto por meio do aplicativo Web Access

É possível usar o aplicativo Web Access para se conectar a um ambiente remoto implementado nas infraestruturas do Citrix Workspace. O Web Access é compatível com HTML5 e fornece uma conexão HTTPS segura ao conectar.

Todos os dados necessários para sessões remotas, como arquivos de cookie, serão mantidos no thin client até que a sessão remota seja encerrada. Depois disso, os dados serão excluídos.

Para se conectar a um ambiente remoto pelo aplicativo Web Access:

1. [Ativar o Kaspersky Thin Client](#).

2. No desktop do Kaspersky Thin Client, clique no botão **Web Access**.

3. Na janela de conexão exibida, forneça o endereço do servidor do ambiente remoto necessário no campo **Servidor**.

4. Pressione **Enter** ou clique em **Conectar**.

Você verá uma janela solicitando que adicione um certificado para se conectar ao ambiente remoto se as condições a seguir forem atendidas:

- Você está se conectando a um ambiente remoto na interface do Kaspersky Thin Client pela primeira vez.
- O thin client está em um dos seguintes estados:
 - não conectado ao Kaspersky Security Center
 - não adicionado ao [grupo de administração](#) 
 - [nenhum certificado para conexão ao ambiente remoto foi adicionado](#) para o grupo de administração ao qual o thin client pertence

Verifique as configurações do certificado e clique no botão **Adicionar certificado**. O certificado será adicionado ao armazenamento de certificados do sistema do Kaspersky Thin Client e será usado para conexões subsequentes.

A janela de entrada de dados de conexão é exibida.

5. Insira o nome de usuário e a senha para se conectar ao ambiente remoto.

O sistema não salva as credenciais para se conectar a um ambiente remoto implementado em uma infraestrutura Citrix Workspace, portanto, é necessário inseri-las sempre que iniciar uma sessão remota.

Caso um desktop remoto esteja disponível, ele será exibido na tela, e em seguida, será possível começar a trabalhar no ambiente remoto. Se vários desktops remotos estiverem disponíveis, você verá uma janela contendo uma lista delas.

6. Para atualizar a lista de desktops remotos, clique no botão **Recarregar**.

7. Clique no botão com o nome do desktop remoto ao qual deseja se conectar.

Uma janela do ambiente remoto ao qual você está conectado será exibida. Uma [sessão remota](#) será iniciada.

Gerenciamento de uma sessão remota

Esta seção contém informações sobre como gerenciar uma [sessão remota](#) na interface do Kaspersky Thin Client usando o painel de conexão e as [teclas de atalho](#).

Uso do painel de conexão

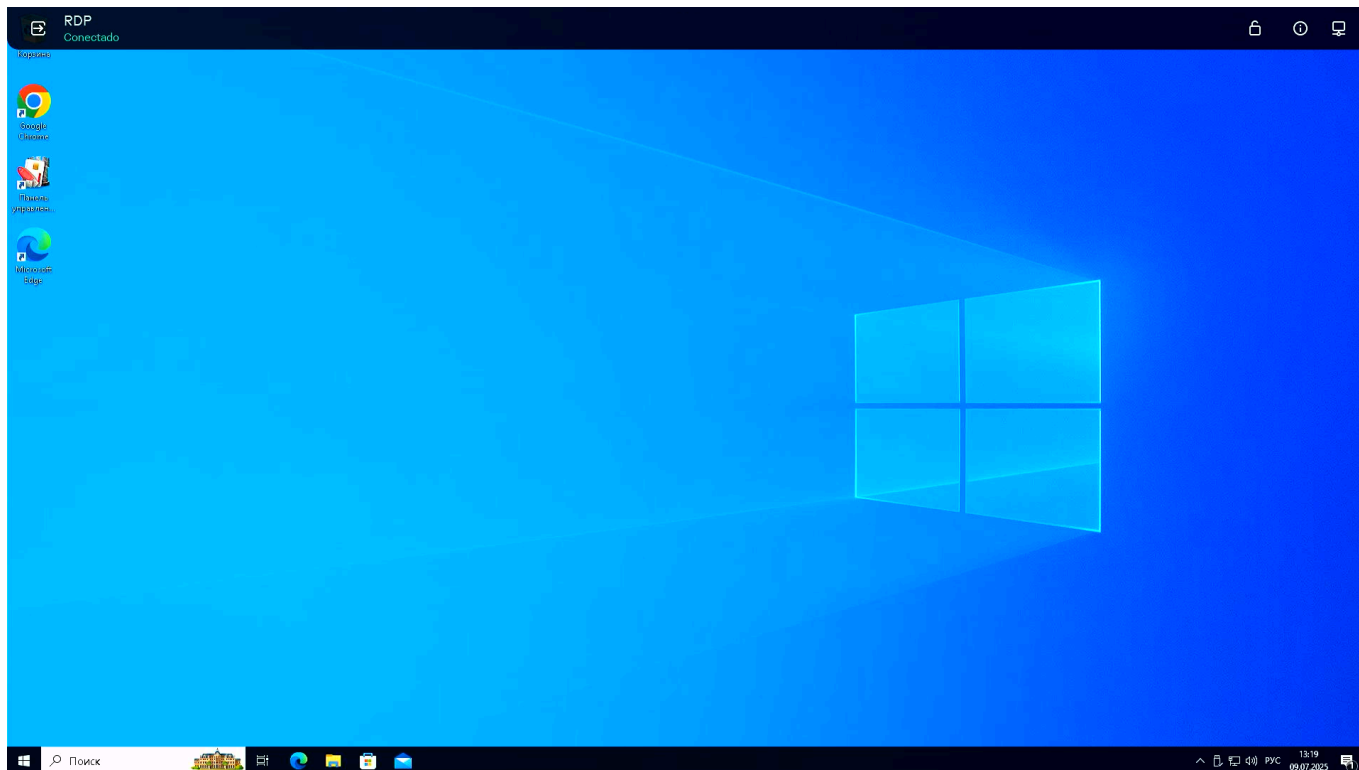
O painel de conexão (doravante também chamado "o painel") é exibido na parte superior da tela após a conexão bem-sucedida com um ambiente remoto. É utilizado para gerenciar a [sessão remota](#) ativa.

Estados do painel de conexão

O painel de conexão pode estar em um dos seguintes estados:

- Expandido.

O painel é totalmente exibido na parte superior da tela da sessão remota (veja a figura abaixo).



Janela que mostra uma sessão remota em execução com o painel de conexão expandido

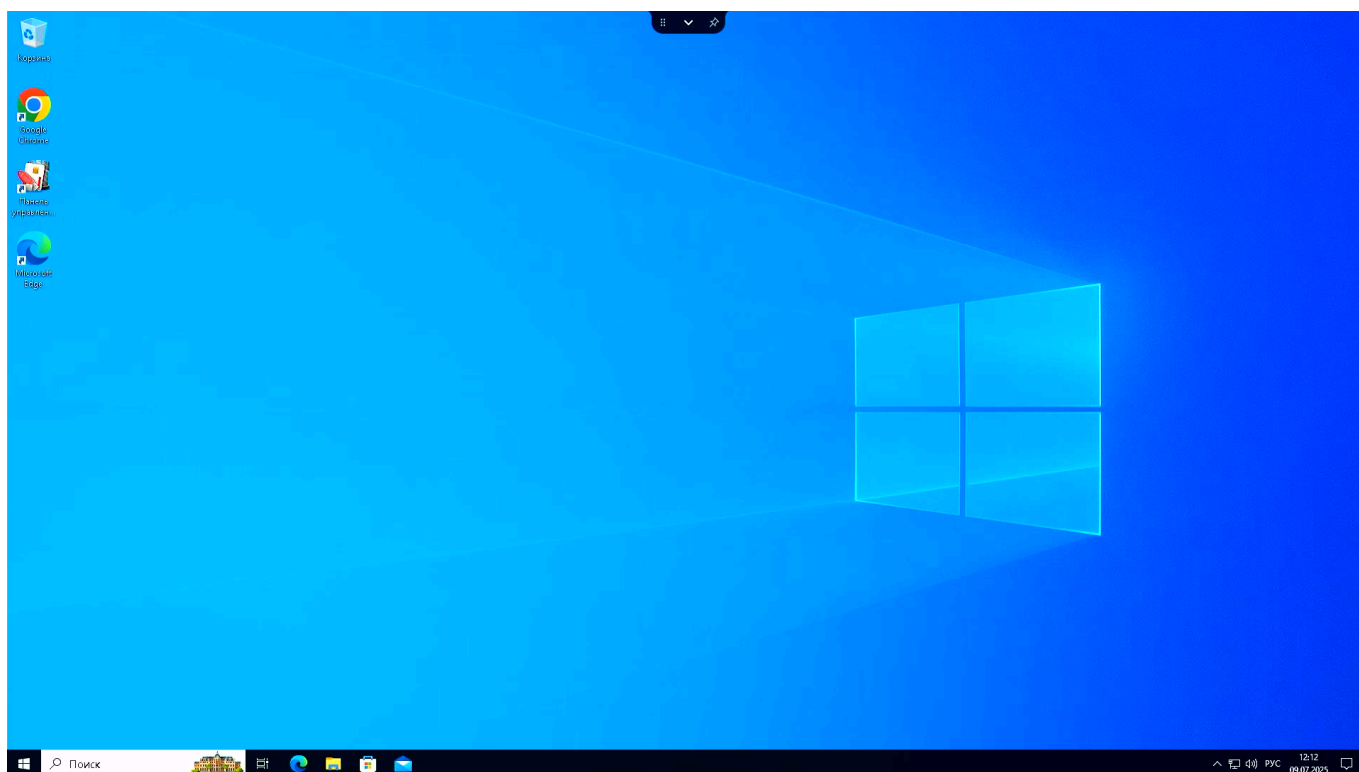
- Oculto.

O painel não é exibido na tela.

Caso o painel de conexão não esteja fixado, ele será recolhido automaticamente quando estiver fora do foco do teclado ou mouse.

- Recolhido.

Os elementos de controle do painel de conexão são exibidos quando se passa o cursor sobre a parte superior da tela (veja a figura abaixo).



Janela que mostra uma sessão remota em execução com o painel de conexão recolhido

Alterar o estado do painel de conexão

Na interface do Kaspersky Thin Client, é possível alterar o estado do painel de conexão e também mover o painel recolhido horizontalmente para fixá-lo em qualquer lugar na tela.

É possível alterar o estado do painel de conexão da seguinte forma:

- Caso queira ocultar completamente o painel de conexão expandido, execute uma das seguintes ações:
 - pressione **CTRL+ALT+HOME** ou **ESC**
 - clique em qualquer área da tela fora do painel
- Caso queira exibir um painel de conexão recolhido, passe o cursor sobre a parte superior da tela. Os elementos de controle do painel serão exibidos.
- Caso queira expandir o painel de conexão, execute uma das seguintes ações:
 - pressione **CTRL+ALT+HOME**
 - restaure o painel de conexão recolhido e clique no botão 

É possível gerenciar um painel de conexão minimizado das seguintes formas:

- Caso queira alterar a posição do painel, clique e segure o botão  e mova o painel para a direita ou para a esquerda.
- Caso queira fixar um painel recolhido em sua posição atual, clique no botão . O painel de conexão será exibido em seu estado recolhido na parte superior da tela até que ele seja ocultado ou desmarcado.
- Caso precise desafixar o painel, clique no botão .

A posição do painel recolhido na tela é salva para as conexões futuras, mesmo depois que o thin client seja reiniciado ou encerrado.

Bloqueio e desbloqueio de sessão remota

O Kaspersky Thin Client bloqueia automaticamente as sessões remotas quando a tela é desligada após o tempo de inatividade [definido nas configurações do thin client](#). Também é possível bloquear e desbloquear uma sessão remota manualmente.

Para bloquear uma sessão remota em andamento,

pressione **Win+L** ou [expanda o painel de conexão](#) e clique em .

A sessão remota será bloqueada. Uma tela de bloqueio será exibida.

Para encerrar uma sessão remota bloqueada:

1. Mova o mouse ou pressione qualquer tecla.
2. Na tela exibida, clique em **Encerrar a sessão remota**.

A sessão remota será encerrada e a janela do aplicativo em que a sessão remota foi iniciada será exibida.

Para desbloquear uma sessão remota:

1. Mova o mouse ou pressione qualquer tecla.
2. Na tela exibida, digite a senha utilizada para se conectar ao sistema remoto.

Se a autenticação inicial foi realizada com um [broker](#) ou outro serviço de conexão remota, será necessário digitar a mesma senha utilizada para se conectar a esse serviço.

3. Clique em **Desbloquear**.

A sessão remota será desbloqueada. A tela do ambiente remoto será exibida.

Encerramento de uma sessão remota

Para encerrar uma sessão remota,

[restaure o painel de conexão](#) e clique em  ou pressione **CTRL+D**.

A sessão remota será encerrada e uma janela de conexão será exibida.

Gerenciamento de dispositivos de reprodução e gravação de áudio em um painel de conexão

É possível conectar diversos dispositivos de reprodução e gravação de áudio a um thin client que executa o Kaspersky Thin Client por um miniconector ou uma porta USB para redirecioná-los ao ambiente remoto. Na interface do Kaspersky Thin Client, é possível [alternar entre dispositivos conectados](#).

O volume do áudio e outras configurações são gerenciados no ambiente remoto.

Não há suporte para o redirecionamento de mais de dois dispositivos USB simultaneamente ao se conectar com um ambiente remoto implementado na infraestrutura do Citrix Workspace.

A conexão por meio de miniconector não é compatível com thin clients Dell Wyse 3040.

Para seleccionar dispositivos de reprodução e gravação de áudio em uma sessão remota:

1. [Restaure o painel de conexão](#) e clique no botão  no painel aberto.
2. Na janela aberta, selecione o dispositivo de reprodução de áudio na lista **Saída** e o dispositivo de gravação de áudio na lista **Entrada**.

Se o dispositivo desejado não estiver na lista, verifique as configurações de redirecionamento no aplicativo usado para se conectar ao ambiente remoto ou entre em contato com o administrador da sua empresa.

Gerenciamento de janelas de aplicativos virtuais

Ao se conectar a um [aplicativo virtual](#), é possível alternar entre as janelas no painel de conexão do Kaspersky Thin Client.

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

1. Restaure o painel de conexão.
2. Clique no ícone do aplicativo.
Uma lista de janelas de aplicativos abertas será exibida.
3. Clique na janela pertinente.
A janela do aplicativo virtual selecionado será exibida.

Web Access: redirecionamento de dispositivos USB para um ambiente remoto

É possível redirecionar impressoras, scanners, webcams e unidades USB para um ambiente remoto implementado em uma infraestrutura Citrix Workspace. O redirecionamento da webcam não requer configuração adicional no ambiente remoto.

Não mais do que dois [dispositivos USB](#) podem ser redirecionados ao mesmo tempo.

Redirecionamento de uma impressora ou um scanner para um ambiente remoto

Para redirecionar uma impressora ou um scanner para um ambiente remoto:

1. Conecte o dispositivo ao thin client por meio do conector USB.
2. Caso esteja conectando um scanner, [especifique manualmente o tipo de dispositivo](#) em **Configurações -> Dispositivos USB não reconhecidos**.
3. [Conecte-se com um ambiente remoto no aplicativo Web Access](#).

4. Expanda o painel de controle do Citrix Workspace na parte superior da janela e clique no botão **USB Devices**.
Uma janela ficará visível para solicitar o redirecionamento do dispositivo USB.
5. Clique em **Adicionar**.
Uma janela ficará visível exibindo uma lista de dispositivos disponíveis para redirecionamento.
6. Caso o dispositivo pertinente não apareça na lista, tente reiniciar a sessão remota sem remover o dispositivo USB.
7. Selecione o dispositivo pertinente na lista e clique em **Conectar**.
O dispositivo será redirecionado para o ambiente remoto. Agora, é possível usá-lo em um desktop remoto.

Caso precise redirecionar vários dispositivos, repita as etapas 4 a 6 destas instruções para cada um deles.

Para obter mais informações sobre o redirecionamento de dispositivos USB, consulte a [documentação do produto Citrix Workspace](#).

Redirecionamento de dispositivos USB para um ambiente remoto

Também é possível redirecionar unidades USB para o ambiente remoto e removê-las com segurança. O redirecionamento usa a tecnologia de mapeamento da unidade cliente. Para obter mais detalhes, consulte a [documentação do produto Citrix Workspace](#).

Para redirecionar unidades USB para um ambiente remoto implementado em uma infraestrutura Citrix Workspace:

1. Conecte o dispositivo ao thin client por meio do conector USB.
 2. [Conecte-se com um ambiente remoto no aplicativo Web Access](#).
 3. Expanda o painel de controle do Citrix Workspace na parte superior da janela e clique em **Map a drive**.
Será possível visualizar uma janela para selecionar o diretório de montagem.
 4. Clique em **Browse**.
Uma janela de confirmação será exibida.
 5. Clique em **Redirecionar** para confirmar o redirecionamento de todas as unidades USB conectadas ao thin client.
Será possível visualizar uma janela para selecionar o diretório de montagem.
 6. Clique em **Add** para confirmar o redirecionamento.
 7. Encerre a sessão remota para se conectar ao ambiente remoto novamente e concluir o redirecionamento.
- As unidades USB serão redirecionadas para o ambiente remoto. Um disco que contém pastas com os nomes das unidades USB redirecionadas será exibido no sistema de arquivos do ambiente remoto.

Ejetar dispositivos USB com segurança em uma sessão remota

O Kaspersky Thin Client é compatível com a remoção segura de unidades USB em uma sessão remota. Para evitar danos aos dados armazenados no dispositivo, ejete o dispositivo de acordo com as instruções abaixo.

Para ejetar com segurança uma unidade USB em uma sessão remota:

1. [Conecte-se com um ambiente remoto no aplicativo Web Access.](#)
2. [Restaure o painel de conexão](#) e clique no botão .
3. Selecione o dispositivo pertinente ou clique em **Ejetar todas as unidades USB**.
4. Caso seja encontrado um problema com a remoção segura, uma mensagem de erro será exibida. Feche todas as janelas no desktop remoto, encerre os processos de cópia e tente novamente.

Agora, o dispositivo estará pronto para ser removido com segurança e será possível desconectá-lo fisicamente do thin client.

Visualização de informações sobre o Kaspersky Thin Client e um thin client

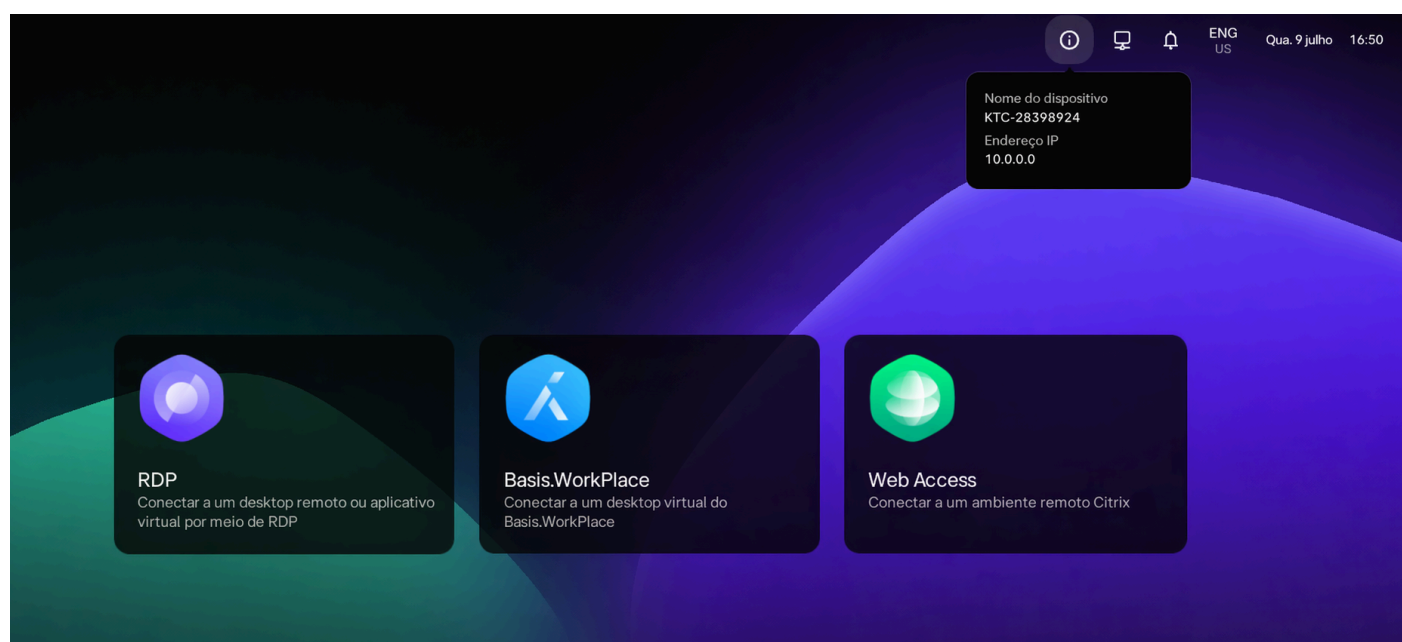
Na interface do Kaspersky Thin Client, é possível visualizar a versão atual do sistema operacional, a data de lançamento e a versão do SDK. A interface também exibe o endereço IP e o nome do thin client.

Para visualizar informações sobre um thin client,

no painel de controle do Kaspersky Thin Client, clique em .

Uma janela contendo informações sobre o thin client é exibida.

Essa janela também exibirá os contatos do Suporte Técnico ou os contatos do administrador de sua empresa se o thin client tiver sido adicionado ao [grupo de administração](#) e se esses dados tiverem sido [especificados na política por meio do Web Console](#).

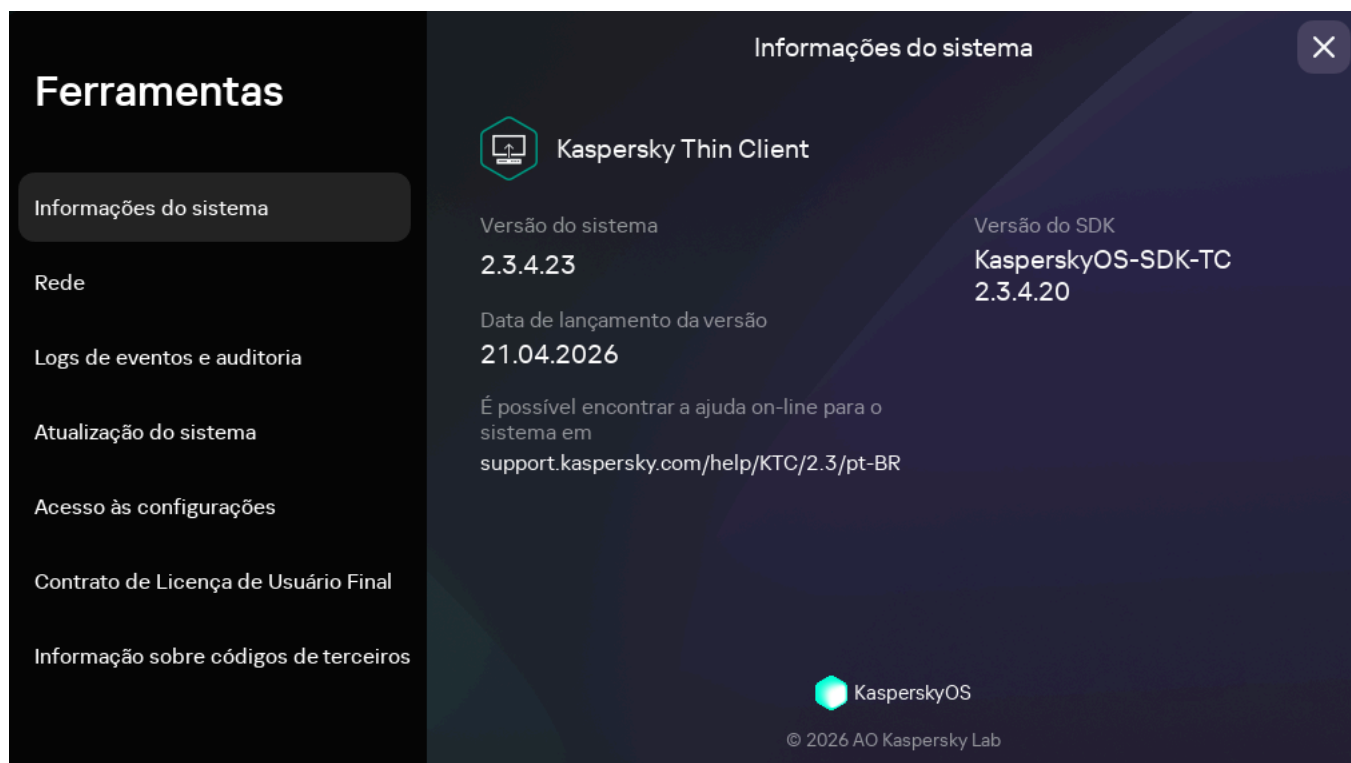


Janela de informações do thin client

Para visualizar as informações sobre o Kaspersky Thin Client,

no painel de controle do Kaspersky Thin Client, clique em  e selecione **Ferramentas** → **Informações do sistema** no menu aberto (veja a figura abaixo).

Será exibida uma janela com informações sobre o Kaspersky Thin Client.



Ferramentas. Seção de Informações do sistema

Exibição das informações do status da rede

Na interface o Kaspersky Thin Client, é possível exibir as configurações para deixar o sistema conectado com a rede e exibir as informações sobre o status da conexão de rede. As informações sobre as configurações de conexão de rede do Kaspersky Thin Client são atualizadas automaticamente pelo menos uma vez a cada segundo.

Para exibir as informações sobre o status da conexão da rede,

no painel de controle do Kaspersky Thin Client, passe o mouse sobre o ícone .

Uma janela contendo as informações sobre o status da conexão de rede será exibida.

Para visualizar as configurações da conexão de rede,

no painel de controle do Kaspersky Thin Client, clique em  e selecione **Ferramentas** → **Rede** no menu aberto (veja a figura abaixo).

Será exibida uma janela que mostra as configurações para conectar o Kaspersky Thin Client à rede (veja a figura abaixo):

- **Endereço MAC:** endereço MAC do dispositivo onde o Kaspersky Thin Client está instalado.
- **Endereço IP:** endereço IP do dispositivo onde o Kaspersky Thin Client está instalado.
- **Máscara de sub-rede:** máscara de sub-rede contendo o endereço IP do dispositivo.
- **Gateway padrão:** endereço do gateway de rede.
- **Servidores DNS:** endereços de servidores DNS. Para visualizar todos os endereços (se houver mais de três), passe o mouse sobre o valor da configuração.
- **Conexão:** status da conexão de rede do Kaspersky Thin Client e a velocidade da conexão.
- **Enviado:** número e tamanho total de pacotes de rede enviados do Kaspersky Thin Client.
- **Recebido:** número e tamanho total de pacotes de rede recebidos pelo Kaspersky Thin Client.

Rede	
Endereço MAC:	50:00:00:00:00:50
Endereço IP:	10.0.0.0
Máscara de sub-rede:	255.255.255.0
Gateway padrão:	10.0.2.2
Servidores DNS:	10.0.2.3
Conexão:	1000 Mbit/s
Enviado:	8 pacotes, 946.00 B
Recebido:	14 pacotes, 2.44 KB

Ferramentas. Seção Rede

Exibição das notificações do Kaspersky Thin Client

A interface do Kaspersky Thin Client exibe os seguintes tipos de notificações:

- Solicita a seleção de uma ação ao clicar em um botão, por exemplo, executar ou adiar uma atualização. Após algum tempo, o Kaspersky Thin Client repetirá todas as solicitações fechadas sem selecionar uma ação. Uma solicitação é considerada resolvida depois que uma ação for selecionada.
- Solicitações para ir para outra seção do Kaspersky Thin Client para definir outras configurações. Por exemplo, o sistema solicita que o usuário configure o layout do monitor quando um segundo monitor é conectado. É possível escolher entre ir para a outra seção do sistema ao clicar no botão apropriado ou dispensar a solicitação.
- Notificações informativas. Essas notificações não exigem a execução de nenhuma ação. Sua única opção é fechar a notificação depois de analisar seu conteúdo.

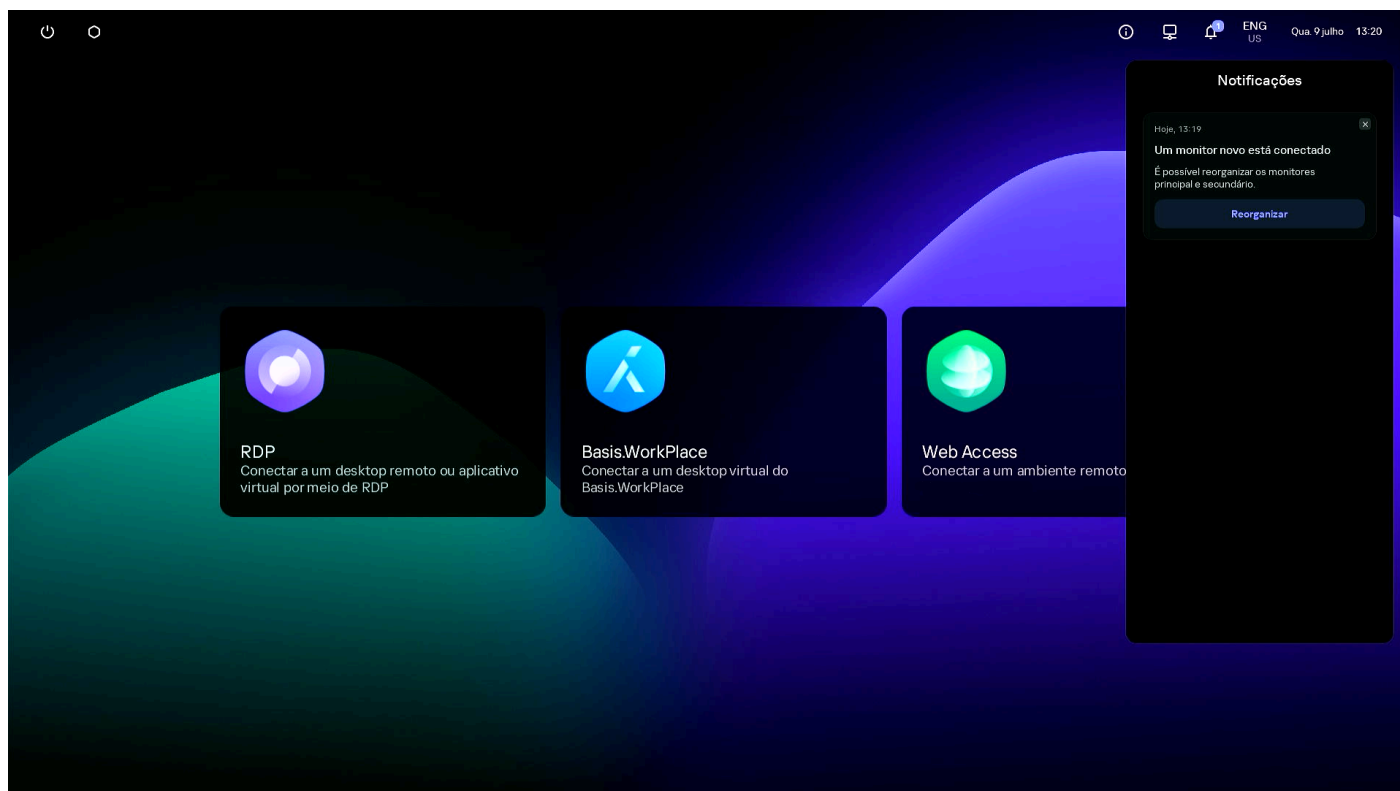
Caso o foco do cursor ou do teclado esteja fora da área de notificação, as solicitações não resolvidas e não lidas serão ocultadas, e o contador no painel de controle exibirá seu número.

As notificações de atualização não são ocultadas automaticamente em sessões remotas. Será necessário descartá-las manualmente ou executar a ação necessária para fazê-las desaparecer.

Para exibir uma lista de todas as notificações do Kaspersky Thin Client,

no [painel de controle](#) do Kaspersky Thin Client, clique em .

O painel de notificações será exibido. Caso tenha novas notificações, elas serão exibidas no painel (veja a figura abaixo).



Painel de notificações do Kaspersky Thin Client

Gerenciamento de certificados na interface do Kaspersky Thin Client

O Kaspersky Thin Client não verifica se o certificado está na lista de revogação de certificados.

Sobre os certificados para conexão com o Kaspersky Security Center

Caso o administrador do Kaspersky Security Center substitua o [certificado para conexão com o Kaspersky Security Center](#), em alguns casos poderá ser necessário fazer a confirmação de sua substituição. Por exemplo, isso pode ser necessário se o thin client tiver sido desativado por muito tempo, não tiver sido sincronizado com o Kaspersky Security Center e o certificado anteriormente usado para conexão com o Kaspersky Security Center tiver expirado.

Para confirmar a substituição do certificado de dispositivos móveis para conexão com o Kaspersky Security Center:

1. Ativar o Kaspersky Thin Client.
2. Na janela aberta **O certificado deve ser substituído**, visualize e memorize o código de confirmação e forneça-o ao administrador do Kaspersky Security Center. Os detalhes de contato do administrador são fornecidos na janela **O certificado deve ser substituído**. O administrador do Kaspersky Security Center envia para o usuário um código de substituição do certificado em resposta.

3. Clique em **Avançar**.

4. Na janela aberta **Código de substituição do certificado**, insira o código fornecido pelo administrador do Kaspersky Security Center e clique no botão **Confirmar**.

Em seguida, o novo certificado para conexão com o Kaspersky Security Center será salvo no armazenamento de certificados do Kaspersky Thin Client. Ele será usado posteriormente para conexão com o Kaspersky Security Center.

Sobre certificados usados para conectar-se a um ambiente remoto e a um servidor de log

Se um thin client não estiver conectado ao Kaspersky Security Center e o administrador não tiver atribuído certificados a ele no Web Console, um usuário também poderá conectar-se a nós e usar certificados que não são controlados pelo administrador. Recomendamos configurar a [conexão de um grupo de administração](#) a um servidor de log e a um ambiente remoto usando somente os certificados atribuídos pelo administrador no Web Console. Essas medidas ajudarão a impedir que o Kaspersky Thin Client se conecte a nós não confiáveis.

Você pode usar ou rejeitar um certificado na interface do Kaspersky Thin Client nos seguintes casos:

- [ao conectar o Kaspersky Thin Client ao Kaspersky Security Center pela primeira vez](#)
- ao se conectar com um ambiente remoto pela primeira vez
- [ao se conectar a um servidor de log pela primeira vez](#)

Os certificados aceitos são salvos no armazenamento do sistema do Kaspersky Thin Client.

Se um thin client estiver incluído em um [grupo de administração](#) e a esse grupo tiverem sido [atribuídos certificados no Web Console](#), você não poderá gerenciar os certificados na interface do Kaspersky Thin Client.

Gerenciamento do Kaspersky Thin Client com o uso de teclas de atalho

É possível utilizar atalhos de teclado dedicados ao trabalhar com o Kaspersky Thin Client e durante [sessões remotas](#). A tabela abaixo lista todas as teclas de atalho e combinações de teclas disponíveis.

Teclas de atalho e combinações de teclas para o Kaspersky Thin Client

Teclas e combinações de teclas	Ações
Win	Abre ou fecha o menu de encerrar .
→ ←	Alterne entre aplicativos (RDP, Basis.WorkPlace, Web Access) no desktop do Kaspersky Thin Client.
↑ ↓	• Alterna entre os itens da lista suspensa. • Rola o conteúdo da página para cima ou para baixo.

Teclas e combinações de teclas	Ações
Tab	Alterna da <i>esquerda</i> para a <i>direita</i> ou de <i>cima</i> para <i>baixo</i> entre as seguintes opções: - Opções de conexão. - A ordem dos campos, por exemplo, na janela Configurações. - Botões no painel de conexão. Ao alternar, os itens indisponíveis, como campos desativados e itens inativos, são ignorados.
Shift+Tab	Alterna da <i>direita</i> para a <i>esquerda</i> ou de <i>baixo</i> para <i>cima</i> entre as seguintes opções: - Opções de conexão. - A ordem dos campos, por exemplo, na janela Configurações. - Botões no painel de conexão. Ao alternar, os itens indisponíveis, como campos desativados e itens inativos, são ignorados.
Espaço ou Enter	- Clica no botão com o foco do teclado nele. - Abre ou fecha a lista suspensa com o foco do teclado nela. Ao alternar, os itens indisponíveis, como campos desativados e itens inativos, são ignorados.
Esc	- Fecha a janela ativa. - Recolhe o painel de conexão com o foco do teclado nele.
Alt+Shift	Altera o idioma do teclado.
Alt+Page down Alt+Page up	Acesse a seção anterior ou a próxima seção da janela Configurações ou Ferramentas. Quando acontece alternância entre as seções, seu estado e o elemento em foco são preservados. Por exemplo, na janela Configurações, quando acontece alternância da seção Geral para a seção Rede, o foco na seção Geral permanece no mesmo campo onde estava quando ocorreu alternância para outra seção.
Ctrl+Alt+Home	Recolhe ou restaura o painel de conexão .
Ctrl+D	Encerra a sessão remota. O atalho só funciona em um painel de conexão expandido.
Win+I	Abra Configurações no desktop do Kaspersky Thin Client caso o acesso às configurações esteja desbloqueado .
Win+U	Abra Ferramentas no desktop do Kaspersky Thin Client.
Win+L	Bloqueia uma sessão remota em andamento.
Win+Esc	Feche o Kaspersky Thin Client pelo desktop do Kaspersky Thin Client.
Win+F12 ou Win+End	Reinicie o Kaspersky Thin Client pelo desktop do Kaspersky Thin Client.
Win+A or Win+N	Abra o painel de notificações no desktop do Kaspersky Thin Client.
Win+↓ Win+↑	Recolhe ou restaura uma janela quando conectado a um aplicativo virtual.
Win+M	Minimiza todas as janelas quando conectado a um aplicativo virtual.
Win+Shift+M	Restaura todas as janelas quando conectado a um aplicativo virtual.

Administração do acesso ao gerenciamento remoto e à tela do ambiente remoto

No Kaspersky Thin Client, é possível aceitar e rejeitar solicitações de acesso ao gerenciamento remoto do thin client e de acesso à tela da [sessão remota](#) em execução nele (doravante também chamada de "tela do ambiente remoto").

Para aceitar ou recusar uma solicitação de acesso ao gerenciamento remoto de dispositivos e à tela do ambiente remoto:

1. [Ative o thin client](#) e certifique-se de que o [dispositivo esteja conectado à rede](#).

Ao tentar se conectar ao Kaspersky Thin Client, o ícone  será exibido no painel de controle. Uma notificação solicitando conexão será exibida no desktop (veja a figura abaixo).



A notificação do desktop do Kaspersky Thin Client contendo uma solicitação para gerenciar remotamente o thin client

2. Execute umas das seguintes ações:

- Clique em **Negar** para impedir o acesso de gerenciamento remoto ao Kaspersky Thin Client.
- Clique em **Permitir** para permitir que o administrador visualize a tela do Kaspersky Thin Client e gerencie as configurações do sistema.

Aceite a solicitação somente se tiver certeza de que a pessoa se conectando ao Kaspersky Thin Client é o administrador da sua empresa.

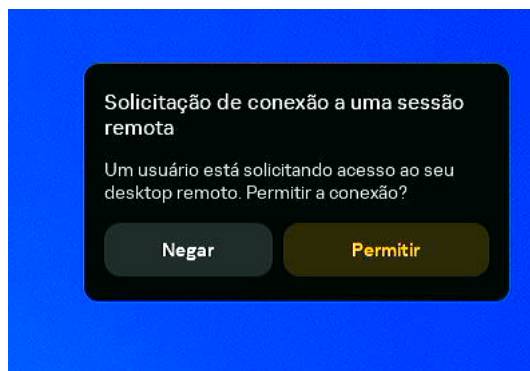
O gerenciamento do Kaspersky Thin Client será transferido para o administrador.

Caso o modo **Permitir automaticamente** esteja configurado [para um dispositivo](#) ou para [seu grupo de administração](#) nas [configurações do Kaspersky Thin Client](#) ou nas configurações de gerenciamento remoto no Web Console e não haja resposta à solicitação em 30 segundos, o gerenciamento do Kaspersky Thin Client será automaticamente transferido para o administrador.

3. Caso uma [sessão remota](#) esteja sendo executada no Kaspersky Thin Client durante a conexão remota ou se uma sessão remota for iniciada pelo administrador durante o gerenciamento remoto do dispositivo, o acesso à tela dessa sessão remota será regulado da seguinte forma:

- Caso a conexão automática à tela remota seja permitida [para o dispositivo](#) ou [seu grupo de administração](#) nas [configurações do Kaspersky Thin Client](#) ou nas configurações de gerenciamento remoto no Web Console, o administrador receberá automaticamente o acesso à tela da sessão remota em execução.
- Caso o modo de acesso à tela do ambiente remoto esteja definido como **Permitir mediante solicitação** nas configurações do Kaspersky Thin Client ou nas configurações de gerenciamento remoto no Web Console, uma notificação contendo uma solicitação para se conectar à sessão remota será exibida na interface do Kaspersky Thin Client (veja a figura abaixo).

O gerenciamento do Kaspersky Thin Client será automaticamente transferido para o usuário.



Notificação que contém uma solicitação de conexão de sessão remota

4. Execute umas das seguintes ações:

- Clique em **Negar** para impedir o acesso do administrador à tela do ambiente remoto.
Caso deseje transferir o gerenciamento do thin client para o administrador novamente, mas sem dar acesso à tela do ambiente remoto, [encerre a sessão remota](#).
- Clique em **Permitir** para permitir que o administrador visualize a tela do ambiente remoto e gerencie a sessão remota.
O gerenciamento do Kaspersky Thin Client será transferido para o administrador.

Conexão remota com um thin client

Um administrador pode se conectar remotamente a um thin client a partir de seu dispositivo com o propósito de gerenciar remotamente o thin client usando um cliente RDP para resolver problemas ou ajudar o usuário a configurar o Kaspersky Thin Client.

Para que o gerenciamento remoto funcione, o thin client deve estar [Ligado](#) e [Conectado à rede](#). O modo de acesso **Permitir automaticamente** ou **Permitir mediante solicitação** do gerenciamento remoto não deve ser definido para o [thin client](#) ou seu [grupo de administração](#) nas [configurações do Kaspersky Thin Client](#) ou nas configurações de gerenciamento remoto no Web Console.

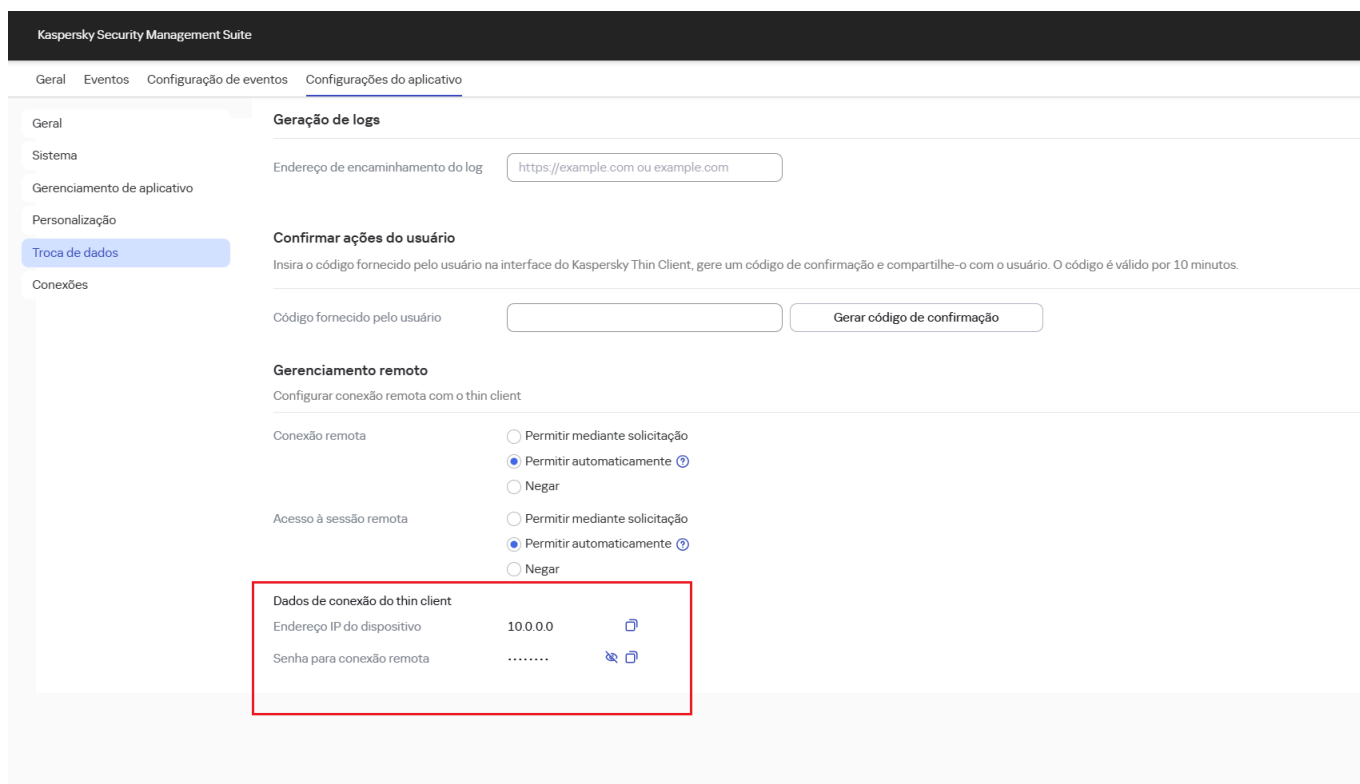
O endereço IP do thin client e a senha de conexão remota (doravante também chamados de "credenciais") são necessários para o gerenciamento remoto.

Para se conectar a um thin client para fins de gerenciamento remoto:

1. Abra o cliente RDP no dispositivo do qual se conectará ao thin client.
2. Obtenha as credenciais de conexão remota por meio de uma das seguintes maneiras:
 - Se o thin client estiver [conectado com o Kaspersky Security Center](#), copie as credenciais na interface do Web Console:
 - a. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**, caso deseje se conectar a um dispositivo de um grupo de administração, ou **Descoberta e implementação** → **Dispositivos não atribuídos**, caso deseje se conectar a um dispositivo que não faça parte de nenhum grupo de administração.
 - b. Na lista aberta, clique no [nome do thin client](#) ao qual deseja se conectar.
 - c. Na janela aberta, selecione a guia **Aplicativos**.
 - d. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
 - e. Na janela aberta, selecione a guia **Configurações do aplicativo**.
 - f. Vá para a seção **Troca de dados**.

g. No bloco **Dados de conexão do thin client**, copie as credenciais da conta de conexão remota ao clicar no botão  ao lado deles (veja a figura abaixo).

A senha para conexão remota no Web Console é atualizada uma vez por dia e após cada reinicialização do thin client.



Janela de configuração para gerenciamento remoto de um thin client no Web Console

- Caso o thin client não esteja conectado com o Kaspersky Security Center, solicite a senha padrão para o [Suporte Técnico](#) e [obtenha o endereço IP do dispositivo na interface do Kaspersky Thin Client](#).

A senha padrão é para uso temporário. Use a senha somente se o thin client ainda não estiver conectado ao Kaspersky Security Center.

3. No cliente RDP instalado em seu dispositivo, insira as credenciais recebidas e inicie a conexão com o thin client.
4. Para se conectar ao thin client, dependendo do modo de acesso de gerenciamento remoto específico e definido nas [configurações do Kaspersky Thin Client](#) ou nas configurações de gerenciamento remoto no Web Console [para o dispositivo](#) ou seu [grupo de administração](#), execute uma das seguintes ações:

- Se o modo **Permitir automaticamente** estiver definido, aguarde até que a conexão com o thin client seja estabelecida.

O usuário pode aceitar ou rejeitar a solicitação em 30 segundos. Caso o usuário não execute nenhuma ação durante esse período, a conexão será iniciada automaticamente.

- Se o modo **Permitir mediante solicitação** estiver definido, aguarde até que o usuário [aceite a solicitação de gerenciamento remoto na interface do Kaspersky Thin Client](#).

Caso tenha se conectado com êxito ao thin client, a janela de acesso à tela do ambiente remoto será exibida.

5. Para obter acesso à tela do ambiente remoto, dependendo do modo de definição que o [Kaspersky Thin Client está configurado](#) ou das configurações de gerenciamento remoto no Web Console [para o dispositivo](#) ou seu [grupo de administração](#), execute uma das seguintes ações:

- Se o modo **Permitir automaticamente** estiver definido, aguarde até que a conexão com o thin client seja estabelecida.
- Caso o modo **Permitir mediante solicitação** estiver definido, aguarde até que o usuário aceite a solicitação na interface do Kaspersky Thin Client ou [encerre a sessão remota](#).
- Se o modo **Negar** estiver definido, aguarde até que o usuário encerre a sessão remota.

A interface do Kaspersky Thin Client é exibida. Você terá acesso ao gerenciamento remoto do Kaspersky Thin Client.

Para encerrar o gerenciamento remoto do thin client na interface do Kaspersky Thin Client,

no [painel de conexão](#), clique no botão . Na janela aberta, clique em **Encerrar**.

Gerenciamento do Kaspersky Thin Client pelo Kaspersky Security Center Web Console

O Kaspersky Security Center Web Console (daqui em diante denominado apenas “Web Console”) é um aplicativo da web criado para possibilitar a execução central das principais tarefas de gerenciamento e manutenção do sistema de segurança de uma rede corporativa. O Web Console é um componente do Kaspersky Security Center que fornece uma interface do usuário. Para obter informações detalhadas sobre o Kaspersky Security Center Web Console consulte a [Ajuda On-line do Kaspersky Security Center](#).

O Kaspersky Thin Client 2.3 é compatível com o Kaspersky Security Center Linux versão 15.3 e o Kaspersky Security Center Web Console versão 15.3.

Sobre o plug-in da Web do Kaspersky Security Management Suite

O *plug-in da Web do Kaspersky Security Management Suite* (também denominado “plug-in da Web”) é um componente especializado que fornece a capacidade de gerenciar a operação do Kaspersky Thin Client pelo Kaspersky Security Center Web Console.

O plug-in da Web permite executar as seguintes operações de forma centralizada:

- gerencie as configurações do Kaspersky Thin Client [para um](#) ou [mais thin clients](#) em um [grupo de administração](#)
- [configure o recebimento de eventos do Kaspersky Thin Client e visualize-os](#)
- [gerenciar certificados de segurança do Kaspersky Thin Client](#)

Para ativar a interação entre o Kaspersky Thin Client e o Kaspersky Security Center, as seguintes condições devem ser atendidas:

- [especifique as configurações de conexão do Kaspersky Security Center](#) ao configurar o Kaspersky Thin Client
- [instale o plug-in da web do Kaspersky Security Management Suite](#) no Kaspersky Security Center

Para garantir a operação estável das funções do sistema e o acesso a todos os seus recursos, as versões principais do plug-in da web do Kaspersky Security Management Suite e do Kaspersky Thin Client devem corresponder.

Instalação do plug-in da Web do Kaspersky Security Management Suite

O Kaspersky Security Management Suite, o Kaspersky Security Center e o Kaspersky Security Center Web Console não estão incluídos no kit de distribuição do Kaspersky Thin Client. Eles devem ser instalados separadamente.

É possível visualizar a lista de plug-ins da Web instalados na interface do Web Console (**Configurações do console** → **Plug-ins da web**).

A funcionalidade do plug-in da Web está disponível para todos os administradores com acesso de navegador ao Web Console. Se necessário, você pode [configurar o controle de acesso para a funcionalidade do Kaspersky Security Management Suite](#).

Caso queira usar a porta padrão para conectar o thin client ao Kaspersky Security Center, a porta 13292 deve estar disponível no Servidor de Administração do Kaspersky Security Center. Caso queira usar uma porta diferente da 13292, será preciso definir as permissões adequadamente. Para obter mais informações sobre a ativação de uma porta no Servidor de Administração do Kaspersky Security Center, consulte a [Ajuda on-line do Kaspersky Security Center](#) ².

Para garantir a operação estável das funções do sistema e o acesso a todos os seus recursos, as versões principais do plug-in da web do Kaspersky Security Management Suite e do Kaspersky Thin Client devem corresponder.

Para instalar o plug-in da Web no Web Console:

1. Abra o arquivo relevante que contém as imagens de instalação do plug-in da Web e os arquivos de assinatura incluídos no [kit de distribuição do Kaspersky Thin Client](#).

O Contrato de Licença de Usuário Final é exibido.

2. Leia o Contrato de Licença de Usuário Final e aceite-o se concordar com os termos nele contidos.

O arquivo relevante que contém imagens de instalação do plug-in da Web e arquivos de assinatura é descompactado automaticamente depois que você aceita o contrato.

3. No menu do Web Console, selecione **Configurações do console** → **Plug-ins da web**.

Uma lista de plug-ins disponíveis do Web Console será exibida.

4. Clique no botão **Adicionar do arquivo**.

5. No painel exibido, adicione os arquivos do arquivo descompactado que contém as imagens de instalação do plug-in da Web e os arquivos de assinatura:

- arquivo ZIP que contém o pacote de distribuição do plug-in (`plugin.zip`) clicando em **Carregar arquivo ZIP**;
- arquivo de assinatura (`signature.txt`), clicando em **Carregar assinatura**.

6. Clique no botão **Adicionar**.

7. Quando a instalação do plug-in da Web for concluída, clique em **OK**.

O plug-in da Web do Kaspersky Security Management Suite será carregado na configuração padrão e aparecerá na lista de plug-ins de gerenciamento do Web Console.

Atualização do plug-in da Web do Kaspersky Security Management Suite

Para atualizar o Kaspersky Security Management Suite, obtenha um arquivo compactado contendo o pacote de instalação do plug-in da Web e uma assinatura digital de arquivo compactado da Kaspersky.

Para atualizar o plug-in da Web no Web Console:

1. Abra o arquivo compactado que contém as imagens de instalação do plug-in da Web e os arquivos de assinatura recebidos da Kaspersky.

O Contrato de Licença de Usuário Final é exibido.

2. Leia o Contrato de Licença de Usuário Final e aceite-o se concordar com os termos nele contidos.

O arquivo relevante que contém imagens de instalação do plug-in da Web e arquivos de assinatura é descompactado automaticamente depois que você aceita o contrato.

3. No menu do Web Console, selecione **Configurações do console** → **Plug-ins da web**.

4. Na lista exibida de plug-ins do Web Console, localize o Kaspersky Security Management Suite e clique nele.

5. Na janela aberta, clique no botão **Atualizar a partir do arquivo**.

6. No painel exibido, adicione os arquivos do arquivo descompactado que contém as imagens de instalação do plug-in da Web e os arquivos de assinatura:

- arquivo ZIP que contém o pacote de distribuição do plug-in (`plugin.zip`) clicando em **Carregar arquivo ZIP**;
- arquivo de assinatura (`signature.txt`), clicando em **Carregar assinatura**.

7. Clique em **Atualizar**.

8. Depois que a atualização for concluída e uma mensagem confirmando a instalação bem-sucedida da atualização for exibida, clique em **OK**.

O plug-in da Web do Kaspersky Security Management Suite será atualizado, e suas informações sobre a versão e a hora de atualização serão exibidas na tabela de plug-ins no Web Console.

Remoção do plug-in da Web do Kaspersky Security Management Suite

O plug-in da Web do Kaspersky Security Management Suite pode ser removido do Web Console. Depois que o plug-in da Web for removido, não será possível gerenciar o Kaspersky Thin Client pela interface do Web Console.

Antes de remover o plug-in da web, exclua os dispositivos gerenciados dos [grupos de administração](#).

Para remover o plug-in da Web do Kaspersky Security Management Suite do Web Console:

1. No menu do Web Console, selecione **Configurações do console** → **Plug-ins da web**.
Uma lista de plug-ins disponíveis do Web Console será exibida.
2. Na lista de plug-ins, marque a caixa de seleção ao lado do plug-in da web do Kaspersky Security Management Suite.
3. Clique no botão **Excluir**.
4. Na janela de confirmação de remoção do plug-in aberta, execute uma das seguintes ações:
 - Caso seja necessário salvar uma cópia de backup do plug-in, clique em **OK**.
Uma cópia de backup do plug-in será criada. O plug-in da Web do Kaspersky Security Management Suite será removido do Web Console.
 - Caso não seja necessário salvar uma cópia de backup do plug-in, clique no botão **Dispensar backup**.
O plug-in da Web do Kaspersky Security Management Suite será removido do Web Console.
5. Na janela aberta que contém as informações sobre a remoção do plug-in, clique em **OK**.

Restrição de acesso às funções do plug-in da Web do Kaspersky Security Management Suite

Caso um usuário do Kaspersky Security Center não tenha [direitos de acesso suficientes às funções do aplicativo](#) ou a função [padrão do Kaspersky Security Center](#) não tenha sido atribuída, o usuário não poderá trabalhar no Kaspersky Security Center Web Console.

É possível configurar os direitos de acesso ao usuário do Kaspersky Security Center às funções do aplicativo das seguintes maneiras:

- configure os direitos de cada usuário ou grupo de usuários separadamente
- crie funções padrão do Kaspersky Security Center com conjuntos de direitos pré-configurados e atribua essas funções aos usuários, dependendo de suas obrigações

Uma *função* é um conjunto pré-configurado de direitos para acessar as funções do Kaspersky Security Management Suite que podem ser atribuídas aos usuários. Recomendamos configurar os direitos de acesso à função de acordo com as tarefas e deveres típicos dos usuários. Depois que um usuário recebe uma função, ele obtém acesso às funções necessárias para cumprir suas obrigações.

Para obter detalhes sobre a configuração do acesso baseado em função, consulte a [Ajuda on-line do Kaspersky Security Center](#).

Além das funções padrão do Kaspersky Security Center, é possível atribuir aos usuários as seguintes funções padrão para gerenciar as funções do Kaspersky Thin Client:

- *Diretor de segurança.* Somente o [gerenciamento de certificados](#) é permitido para esta função. É possível atribuir essa função a um funcionário responsável pela segurança das informações em sua empresa.
- *Administrador.* A função tem acesso a todas as funções de gerenciamento do Kaspersky Thin Client por meio do Web Console, exceto o gerenciamento de certificados.
- *Administrador avançado.* Essa função tem acesso a todas as funções de gerenciamento do Kaspersky Thin Client por meio do Web Console. É possível atribuir essa função a um funcionário responsável pelo suporte e administração dos sistemas de informação em sua organização e que também é responsável pela segurança das informações em sua organização.

A tabela abaixo lista as funções de gerenciamento do Kaspersky Thin Client disponíveis para o usuário, dependendo de sua função atribuída. Para funções marcadas com o ícone ✓, as configurações correspondentes do Kaspersky Thin Client podem ser modificadas pelo Web Console. Todas as funções podem visualizar as configurações do Kaspersky Thin Client correspondentes a todas as funções, pelo Web Console.

Funções de gerenciamento do Kaspersky Thin Client disponíveis no Web Console, dependendo da função do usuário

Função	Diretor de segurança	Administrador	Administrador avançado
Gerenciamento de certificados em uma política do Kaspersky Security Management Suite	✓	–	✓
Definição de configurações para conexão com um ambiente remoto em uma política do Kaspersky Security Management Suite	–	✓	✓
Definição de configurações gerais em uma política do Kaspersky Security Management Suite	–	✓	✓
Gerenciamento das configurações do sistema em uma política do Kaspersky Security Management Suite	–	✓	✓
Gerenciamento dos dados do Kaspersky Thin Client em uma política do Kaspersky Security Management Suite	–	✓	✓
Gerenciamento dos aplicativos do Kaspersky Thin Client em uma política do Kaspersky Security Management Suite	–	✓	✓
Definição de configurações personalizadas em uma política do Kaspersky Security Management Suite	–	✓	✓

Fazendo login e logout do Web Console

Para fazer login no Web Console, o endereço da Web e o número da porta do Servidor de Administração do Kaspersky Security Center, especificados durante a instalação (a porta 8080 é usada por padrão), serão necessários. Também é preciso ativar o JavaScript em seu navegador. Para saber quais são os requisitos do navegador do Kaspersky Security Center Web Console, consulte a seção [Requisitos de hardware e software](#) da Ajuda on-line do Kaspersky Security Center.

Para efetuar login no Web Console:

1. Em seu navegador, vá para `https://<endereço do Servidor de Administração>:<Número da porta>`.
A página de login é aberta.
2. Faça login usando o nome de usuário e a senha do domínio.
Caso o Servidor de Administração não responda ou as credenciais da conta sejam inseridas incorretamente, uma mensagem de erro será exibida.

Após o login, o painel de controle aparece e exibe o último idioma e tema que foram usados. É possível navegar pelo Web Console e usá-lo para trabalhar com o Kaspersky Security Center.

Para fazer logout do Web Console:

1. No canto inferior direito da tela, clique no nome de usuário.
2. No menu aberto, selecione **Sair**.

O Web Console é fechado e a página de login é exibida.

Gerenciamento de políticas e grupos de administração

No Web Console, é possível adicionar thin clients que estão executando o Kaspersky Thin Client e estão conectados ao Kaspersky Security Center a um [grupo de administração](#) para [definir as configurações do sistema](#) com o uso de [políticas](#) de maneira centralizada.

Por padrão, imediatamente após a instalação do Kaspersky Security Center, há um grupo na hierarquia de grupos de administração: **Dispositivos gerenciados**. Todos os grupos criados serão seus grupos secundários. Na política criada para o grupo **Dispositivos gerenciados**, é possível configurar dispositivos em todos os grupos de administração. Recomendamos utilizar a política, por exemplo, para [adicionar certificados](#) de maneira centralizada. Para obter mais informações sobre a hierarquia de grupos e políticas, consulte a [Ajuda do Kaspersky Security Center](#).

Esta seção fornece instruções sobre como criar grupos de administração e adicionar thin clients a eles, além de criar e editar políticas. Para mais informações, consulte a [política](#) e seções de [gerenciamento de dispositivos](#) na Ajuda do Kaspersky Security Center.

Criação de um grupo de administração

No Web Console, é possível criar [grupos de administração](#) e adicionar thin clients que estão executando o Kaspersky Thin Client e estão conectados ao Kaspersky Security Center a esses grupos para [definir as configurações do dispositivo](#) utilizando [políticas](#) de maneira centralizada.

Para criar um grupo de administração:

1. Na janela principal do Web Console, vá para **Ativos (dispositivos)** → **Hierarquia de grupos**.
2. Marque a caixa de seleção ao lado do grupo de administração ao qual o novo grupo deverá fazer parte.
Se você ainda não criou grupos de administração, selecione o grupo **Dispositivos gerenciados**.
3. Clique no botão **Adicionar**.
4. No painel que é aberto, digite um novo nome de grupo de administração e clique em **Adicionar**.

O nome de um grupo de administração deve ser único dentro de sua hierarquia.

O novo grupo aparecerá na lista de grupos de administração.

Adição de thin clients ao grupo de administração

Você pode adicionar thin clients que estão executando o Kaspersky Thin Client ao [grupo de administração que você criou](#) ou ao grupo de **Dispositivos gerenciados**.

Para adicionar dispositivos ao grupo de administração:

1. Na janela principal do Web Console, selecione **Descoberta e implementação** → **Dispositivos não atribuídos**.
Uma lista de todos os dispositivos conectados ao Kaspersky Security Center, mas não adicionados a nenhum grupo de administração, será exibida.
2. Marque as caixas de seleção ao lado dos dispositivos que deseja adicionar ao grupo.
3. Clique no botão **Migrar**.
4. No painel que aparece, selecione o grupo de administração.
5. Clique no botão **Migrar**.

Os dispositivos serão adicionados ao grupo de administração selecionado.

Também é possível automatizar a transferência de thin clients para grupos de administração. Para obter mais detalhes, consulte a [Ajuda on-line do Kaspersky Security Center](#).

Criação da política

Para configurar o Kaspersky Thin Client instalado em thin clients em um [grupo de administração](#), crie uma [política](#) para esse grupo no Web Console.

Por padrão, imediatamente após a instalação do Kaspersky Security Center, há um grupo na hierarquia de grupos de administração: **Dispositivos gerenciados**. Todos os grupos criados serão seus grupos secundários. Na política criada para o grupo **Dispositivos gerenciados**, é possível configurar dispositivos em todos os grupos de administração. Recomendamos utilizar a política, por exemplo, para [adicionar certificados](#) de maneira centralizada. Para obter mais informações sobre a hierarquia de grupos e políticas, consulte a [Ajuda do Kaspersky Security Center](#).

Para criar uma política:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Selecione o grupo de administração necessário. Para fazer isso, clique no caminho atual na parte superior da janela e, no painel que se abre, clique no grupo de administração necessário.
3. Clique no botão **Adicionar**.
4. Na lista de aplicativos exibida na janela aberta, selecione o plug-in da web de administração do Kaspersky Thin Client e clique em **Avançar**.
5. Na janela de configuração da nova política, na guia **Geral**, especifique as seguintes configurações:
 - No campo **Nome**, insira o nome da política.
 - No bloco **Status da política**, selecione um dos seguintes status:
 - **Ativo**
A política aplicada atualmente aos dispositivos no grupo de administração. Se essa opção for selecionada, na próxima vez que você sincronizar o Kaspersky Thin Client e o Kaspersky Security Center, essa política ficará ativa. Cada grupo de administração pode ter apenas uma política ativa. Esse status é selecionado por padrão.
 - **Inativo**
A política não aplicada atualmente aos dispositivos no grupo de administração. Se essa opção for selecionada, a política ficará inativa, mas permanecerá na lista de políticas. Será possível ativar uma política inativa posteriormente.
 - **Ausência**
A política é ativada quando o dispositivo sai do perímetro de rede da organização.
 - Ative ou desative as opções no bloco **Herança de configurações**:
 - **Herdar configurações da política principal**
Caso a alternância seja ativada, as configurações da política serão herdadas da política do grupo de nível superior e não poderão ser modificadas.

Por padrão, a opção está ativada.

- **Forçar herança de configurações nas políticas secundárias**

As configurações de política serão propagadas para as políticas de grupos de administração aninhados (políticas secundárias), e no bloco **Herança de configurações**, na seção **Geral** de cada janela de propriedades de políticas secundárias, a opção **Herdar configurações da política principal** será ativada automaticamente.

Quando essa configuração está ativada, as configurações da política secundária não podem ser modificadas.

Por padrão, a opção está desativada.

Para obter mais informações sobre a hierarquia de grupos e políticas, consulte a [Ajuda do Kaspersky Security Center](#).

6. Se você quiser [personalizar outras configurações](#), selecione a aba **Configurações do aplicativo** e faça as alterações necessárias.

7. Clique em **Salvar** na parte inferior da página.

A política está criada e aparecerá na lista de políticas.

Edição de uma política

No Web Console, é possível editar uma [política criada anteriormente](#).

Para alterar uma política:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Selecione a política que precisa ser editada.
3. Na janela de configuração de política aberta, ajuste as [configurações conforme necessário](#) na guia **Geral**.
4. Clique no botão **Salvar** na parte inferior da página.

As mudanças feitas serão salvas e exibidas nas propriedades da política na seção **Histórico de revisões**.

Bloqueio de configurações em uma política

Em cada [política](#), as configurações ajustáveis têm um botão com um ícone de cadeado para ativar/desativar o bloqueio. As posições de alternância disponíveis são descritas na tabela abaixo.

Posições de alternância do bloco de configurações

Estado	Descrição
 Indefinido 	Os valores atribuídos a esta configuração não se aplicam aos dispositivos regidos pela política. O usuário pode alterar esta configuração na interface de usuário do Kaspersky Thin Client.
 Aplicado 	Os valores atribuídos a esta configuração aplicam-se aos dispositivos regidos pela política. O usuário não poderá alterar esta configuração na interface do Kaspersky Thin Client.

Definição das configurações do Kaspersky Thin Client para um dispositivo pelo Web Console

No Web Console, é possível definir as configurações do Kaspersky Thin Client instalado em um thin client. O dispositivo deve estar conectado ao Kaspersky Security Center e deve ser [adicionado a um grupo de administração](#).

Alteração de um ID de thin client pelo Web Console: um dispositivo

No Kaspersky Security Center Web Console, é possível alterar o identificador de um thin client [adicionado a um grupo de administração](#) se um dispositivo com o mesmo nome já existir no grupo de administração.

É possível configurar nomes de dispositivos em um grupo de administração [utilizando políticas](#).

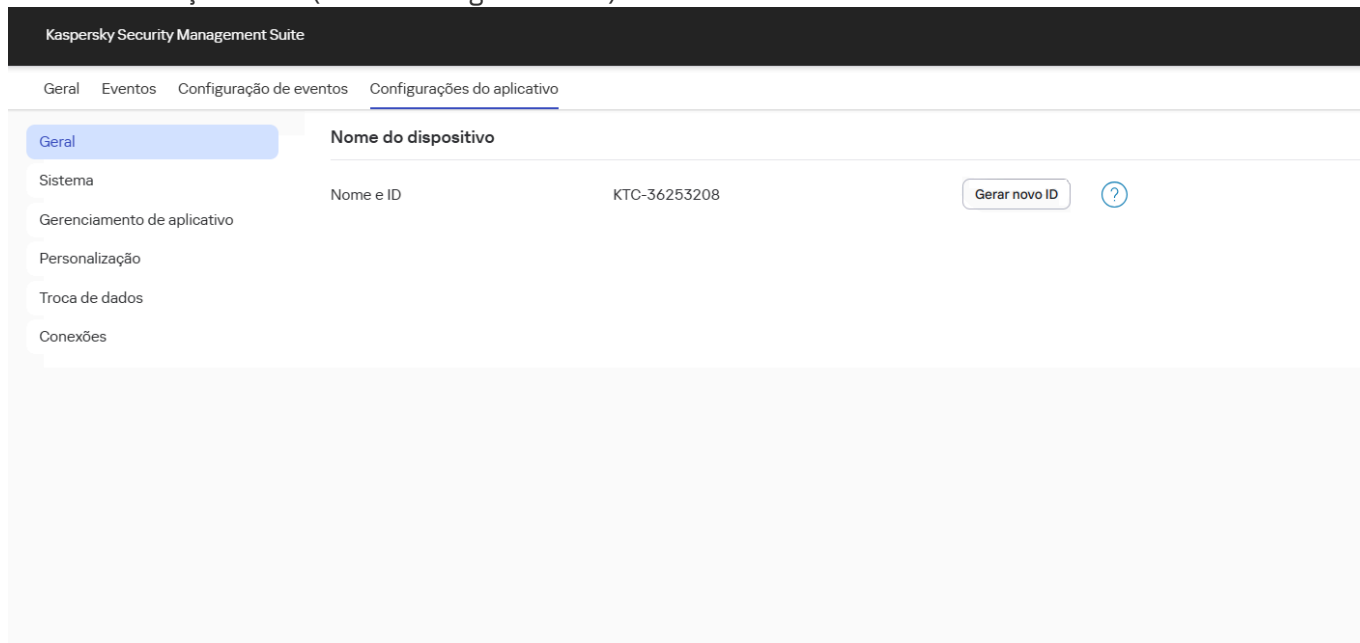
Para alterar um ID de thin client por meio do Web Console:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.
5. Selecione a guia **Configurações do aplicativo**.

6. Selecione a seção **Geral** (consulte a figura abaixo).



Alteração de um ID de thin client por meio do Web Console

7. No grupo **Nome do dispositivo**, clique em **Gerar novo ID**.

Isso inicia o processo de criação de um novo ID. Ele será atualizado na interface do Web Console depois que o thin client for sincronizado com o Kaspersky Security Center.

8. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado em um thin client após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração de uma conexão com um ambiente remoto usando o aplicativo RDP pelo Web Console: um dispositivo

No Web Console, é possível definir as configurações da [conexão a um ambiente remoto pelo aplicativo RDP](#).

Para definir as configurações para a conexão com um ambiente remoto pelo aplicativo RDP:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.

4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.

Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.

5. Selecione a guia **Configurações do aplicativo**.

6. Selecione **Conexões** → **RDP**.

Isso abre uma janela na qual é possível definir as configurações para conexão com um ambiente remoto (veja a figura abaixo).

Janela de configuração para se conectar com um ambiente remoto no aplicativo RDP pelo Web Console

7. No campo **Endereço IP ou nome de servidor**, especifique o endereço IP ou o nome do servidor Microsoft Remote Desktop Connection Broker.

8. No campo **Nome de usuário**, insira o nome da conta de usuário que será usada para a conexão.

9. Caso precise usar o Microsoft Remote Desktop Connection Broker para conexão com um desktop remoto, use o campo **ID da coleta do Remote Desktop Connection Broker** para especificar o ID da coleção no formato `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` refere-se ao identificador específico da coleção).

Caso precise iniciar um aplicativo virtual, especifique o apelido do aplicativo no campo **Apelido do aplicativo**.

Caso tenha um arquivo de configuração contendo as configurações para se conectar com o Microsoft Remote Desktop Connection Broker e, caso seja necessário, o nome do aplicativo a ser aberto, carregue o arquivo clicando em **Carregar arquivo de configuração**. Neste caso, não é necessário preencher os campos **ID da coleta do Remote Desktop Connection Broker** e **Apelido do aplicativo**.

10. Caso queira restaurar automaticamente uma conexão do desktop remoto que foi desconectada inesperadamente, marque a caixa de seleção **Conectar novamente se a conexão for perdida**.

11. No bloco de configurações **Redirecionamento de dispositivos**, selecione os dispositivos a serem redirecionados para o ambiente remoto: **Cartões inteligentes, Unidades USB, Impressoras e outros dispositivos, Microfone, Dispositivos de reprodução de áudio, Câmera da Web (vídeo) e Scanner**.

O volume do áudio e outras configurações são gerenciados no ambiente remoto.

Para redirecionar corretamente os dispositivos USB para um desktop remoto usando o sistema operacional Windows 10, é preciso ativar o Microsoft Remote Desktop Services e permitir o redirecionamento de dispositivos Plug and Play nas configurações do Remote Desktop Services. Para o Microsoft Windows Server 2016 e 2019, é necessário ativar as conexões remotas por meio dos Serviços de Desktop Remoto e permitir a configuração das regras de gerenciamento remoto nesses serviços.

12. No bloco **Qualidade da imagem**, marque as caixas de seleção ao lado das configurações gráficas do desktop remoto que deseja usar: **Fontes suaves**, **Animação do menu**, **Plano de fundo**, **Mostrar o conteúdo das janelas ao arrastar** e **Tema aprimorado**.

Ativar as configurações de exibição do desktop remoto remota poderá afetar a velocidade das operações do Kaspersky Thin Client.

13. Caso dois monitores estejam instalados em sua estação de trabalho e o usuário quiser que uma imagem do desktop remoto seja exibida em ambos os monitores, marque a caixa de seleção **Usar dois monitores** no bloco **Gerenciamento de monitores**.
14. Para melhorar o desempenho quando conectado com desktops remotos ou aplicativos, no bloco **Desempenho**, marque **Melhorar o desempenho gráfico**.

15. Para se conectar a um desktop remoto ou aplicativo virtual automaticamente quando o aplicativo RDP for iniciado, no bloco **Conexão automática**, marque a caixa de seleção **Conectar automaticamente**.

Para ativar a função, o usuário deve se conectar e se desconectar manualmente do ambiente remoto uma vez. Ao fazer isso, os seguintes dados para a conexão com o servidor RDP serão salvos no armazenamento do thin client: nome de usuário, endereço do servidor e senha. Na próxima vez que o aplicativo RDP for iniciado, essas credenciais serão usadas para iniciar automaticamente uma conexão ao ambiente remoto. Caso a função de conexão automática seja desativada, a senha salva será excluída do armazenamento do dispositivo.

O Web Console não permite definir uma senha para se conectar com um ambiente remoto.

Para se conectar automaticamente ao ambiente remoto no aplicativo RDP imediatamente após a inicialização do Kaspersky Thin Client, [configure a inicialização automática do aplicativo](#).

16. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado em um thin client após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração de uma conexão com um ambiente remoto usando o aplicativo Basis.WorkPlace pelo Web Console: um dispositivo

No aplicativo Web Console, é possível definir as configurações para conexão com um ambiente remoto implementado na infraestrutura do Basis.WorkPlace.

Os usuários não podem iniciar uma alteração de senha no Kaspersky Thin Client.

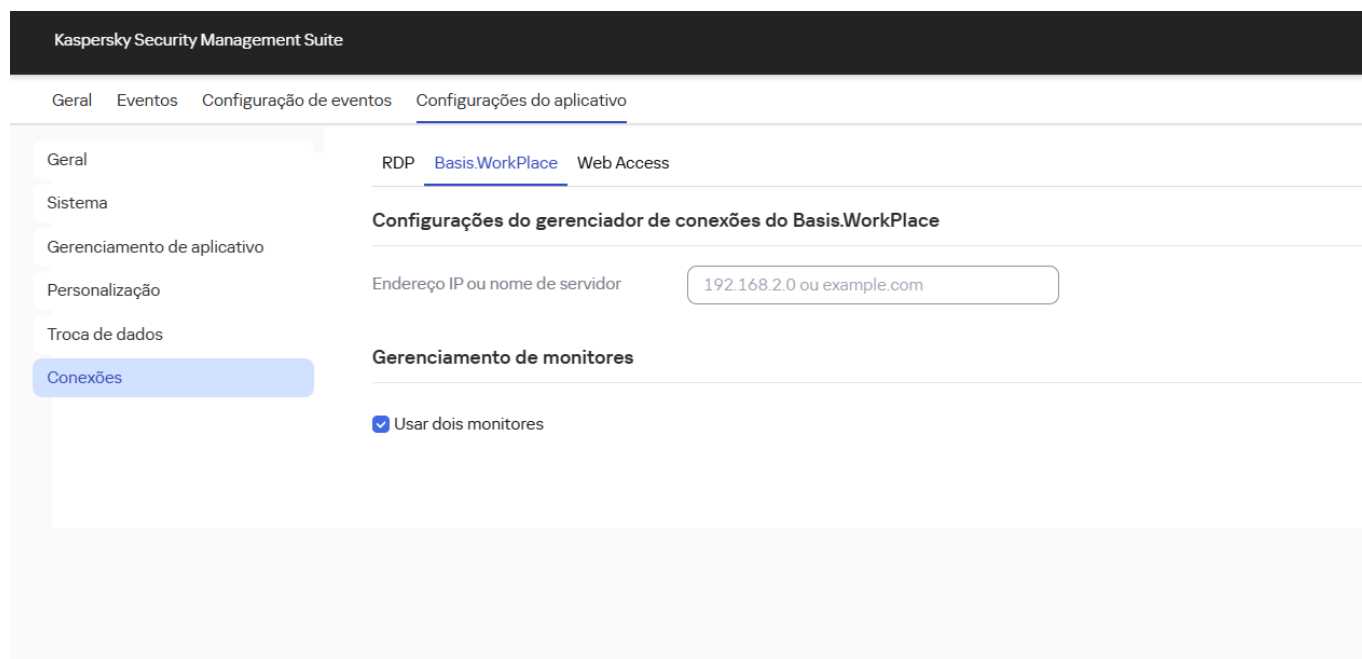
Para definir as configurações de conexão com um ambiente remoto usando a infraestrutura Basis.WorkPlace:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.
5. Selecione a guia **Configurações do aplicativo**.
6. Selecione **Conexões** → **Basis.WorkPlace**.

Isso abre uma janela na qual é possível definir as configurações para conexão com um ambiente remoto (veja a figura abaixo).



Janela de configuração para a conexão com um ambiente remoto implementado no Basis.WorkPlace por meio do Web Console

7. Em **Endereço IP ou nome de servidor**, insira o endereço IP ou o nome do servidor ao qual se conectar.
8. Caso dois monitores estejam instalados em sua estação de trabalho e o usuário quiser que uma imagem do desktop remoto seja exibida em ambos os monitores, marque a caixa de seleção **Usar dois monitores** no bloco **Gerenciamento de monitores**.
9. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado em um thin client após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração de uma conexão com um ambiente remoto no aplicativo Web Access pelo Web Console: um dispositivo

No Web Console, é possível definir as configurações para a [conexão a um ambiente remoto utilizando o aplicativo Web Access](#).

É possível usar o aplicativo Web Access para se conectar a um ambiente remoto implementado nas infraestruturas do Citrix Workspace. O Web Access é compatível com HTML5 e fornece uma conexão HTTPS segura ao conectar.

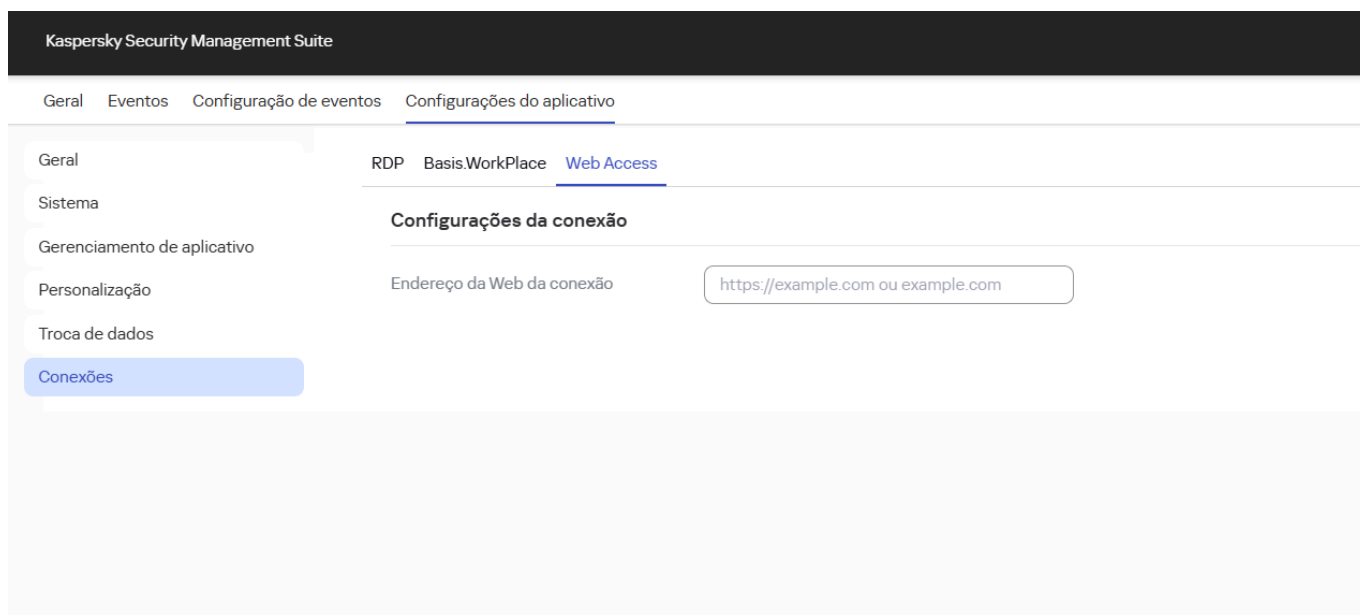
Para definir as configurações para a conexão com um ambiente remoto pelo aplicativo Web Access:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.
5. Selecione a guia **Configurações do aplicativo**.
6. Selecione **Conexões** → **Web Access**.

Isso abre uma janela na qual é possível definir as configurações para conexão com um ambiente remoto (veja a figura abaixo).



7. No campo **Endereço da Web da conexão**, insira o endereço da Web do servidor para se conectar ao [ambiente remoto pertinente](#).

8. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado em um thin client após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração de monitores e telas pelo Web Console: um dispositivo

No Web Console, é possível configurar monitores conectados a um thin client em um [grupo de administração](#) e suas configurações de tela.

O Kaspersky Thin Client é compatível com a conexão de dois monitores. O sistema considera um dos monitores como o principal e o outro como secundário. Durante uma [sessão remota](#), o painel de conexão é exibido na tela do monitor principal. A tela do monitor secundário estende ou duplica a imagem do monitor principal. No Web Console, é possível selecionar qual monitor deve ser considerado o monitor principal (doravante também "alterar o layout do monitor").

Os monitores são numerados na interface do Web Console. O sistema determina os números dos monitores com base na porta de conexão: o monitor 1 é aquele mais próximo da fonte de alimentação e o monitor 2 é o próximo. Consulte a documentação do fabricante do dispositivo para saber a localização das portas nos [modelos de thin client compatíveis](#).

O Web Console não exibe informações sobre quantos monitores estão conectados a um thin client específico.

Se você quiser que a tela da sessão remota seja exibida em ambos os monitores, ative essa opção nas configurações de conexão do ambiente remoto nos aplicativos [RDP](#) ou [Basis.WorkPlace](#).

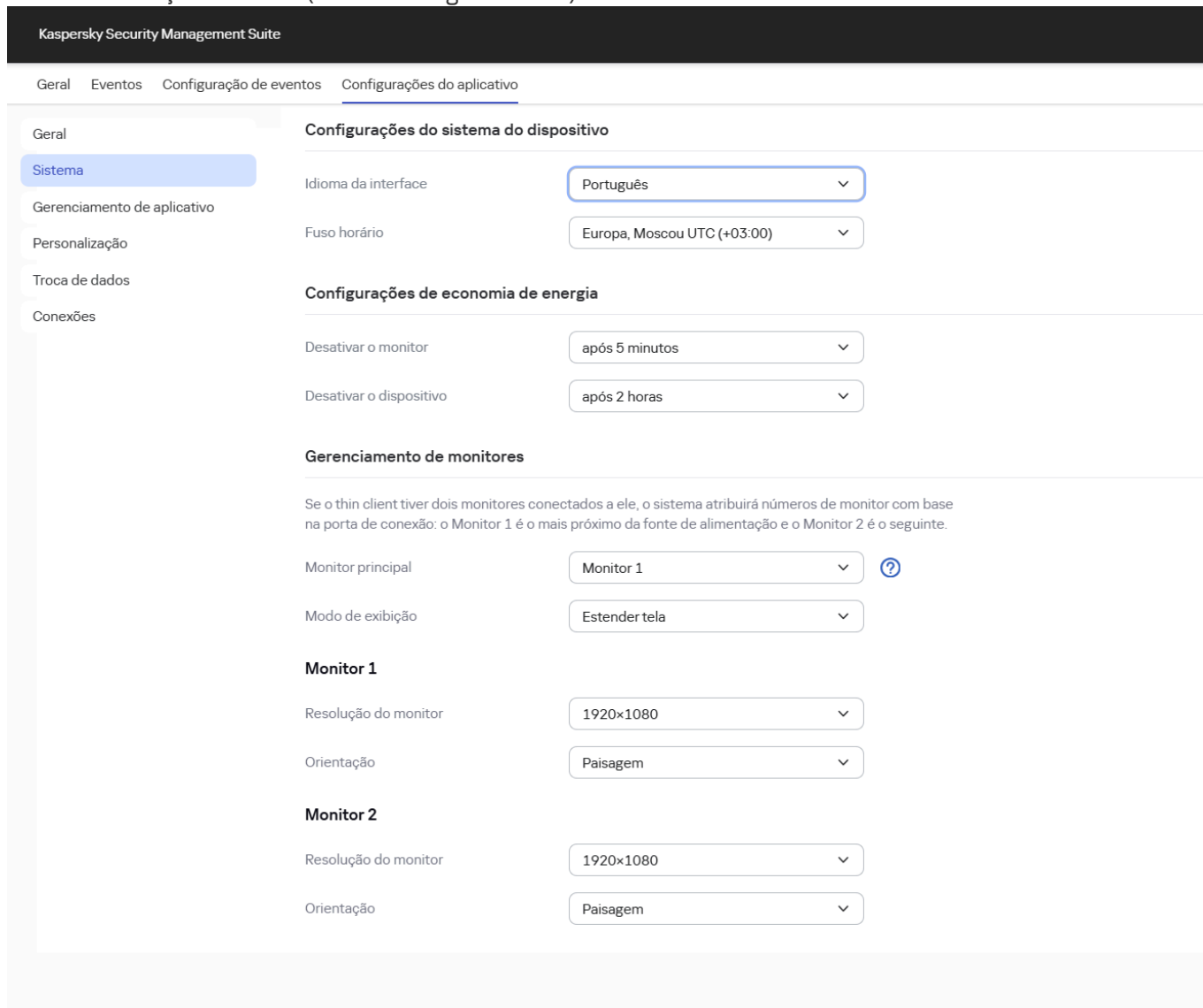
Para configurar monitores e telas pelo Web Console:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.
5. Selecione a guia **Configurações do aplicativo**.

6. Selecione a seção **Sistema** (consulte a figura abaixo).



Kaspersky Security Management Suite

Geral Eventos Configuração de eventos Configurações do aplicativo

Geral

Sistema

Gerenciamento de aplicativo

Personalização

Troca de dados

Conexões

Configurações do sistema do dispositivo

Idioma da interface Português

Fuso horário Europa, Moscou UTC (+03:00)

Configurações de economia de energia

Desativar o monitor após 5 minutos

Desativar o dispositivo após 2 horas

Gerenciamento de monitores

Se o thin client tiver dois monitores conectados a ele, o sistema atribuirá números de monitor com base na porta de conexão: o Monitor 1 é o mais próximo da fonte de alimentação e o Monitor 2 é o seguinte.

Monitor principal Monitor 1 ⓘ

Modo de exibição Estender tela

Monitor 1

Resolução do monitor 1920x1080

Orientação Paisagem

Monitor 2

Resolução do monitor 1920x1080

Orientação Paisagem

Janela de configuração de monitores e telas pelo Web Console:

7. No grupo **Gerenciamento de monitores**, defina as configurações necessárias:

- Na lista suspensa **Monitor principal**, selecione qual deve ser considerado o monitor principal.

Se apenas um monitor estiver conectado ao thin client, as configurações do monitor definido como principal no Web Console serão aplicadas a ele.

- Na lista suspensa **Modo de exibição**, selecione a opção de exibição de imagem:
 - Estender tela**: a imagem se estenderá por dois monitores.
 - Duplicar tela**: a imagem da tela do monitor principal será duplicada no monitor secundário.
- Na lista suspensa **Resolução do monitor**, selecione a resolução desejada para a tela selecionada. As resoluções compatíveis serão listadas [na seção de requisitos de hardware e software](#).

Se o valor **Máxima possível** for selecionado, o valor mais alto do parâmetro compatível com o monitor e com o Kaspersky Thin Client será definido.

- Na lista suspensa **Orientação**, selecione a posição da tela:
 - **Paisagem**: a posição padrão da tela.
 - **Paisagem invertida**: a tela gira 180°.
 - **Retrato**: a tela gira 90°.
 - **Retrato invertido**: a tela gira 270°.

8. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado em um thin client após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Definição das configurações do sistema do Kaspersky Thin Client pelo Web Console: um dispositivo

No Web Console, é possível configurar o idioma da interface e o fuso horário do Kaspersky Thin Client, além de configurar o horário de desligamento para thin clients e seus monitores respectivos.

O Kaspersky Thin Client 2.3 é compatível com os seguintes idiomas de interface: russo, inglês (EUA), espanhol (México) e português (Brasil).

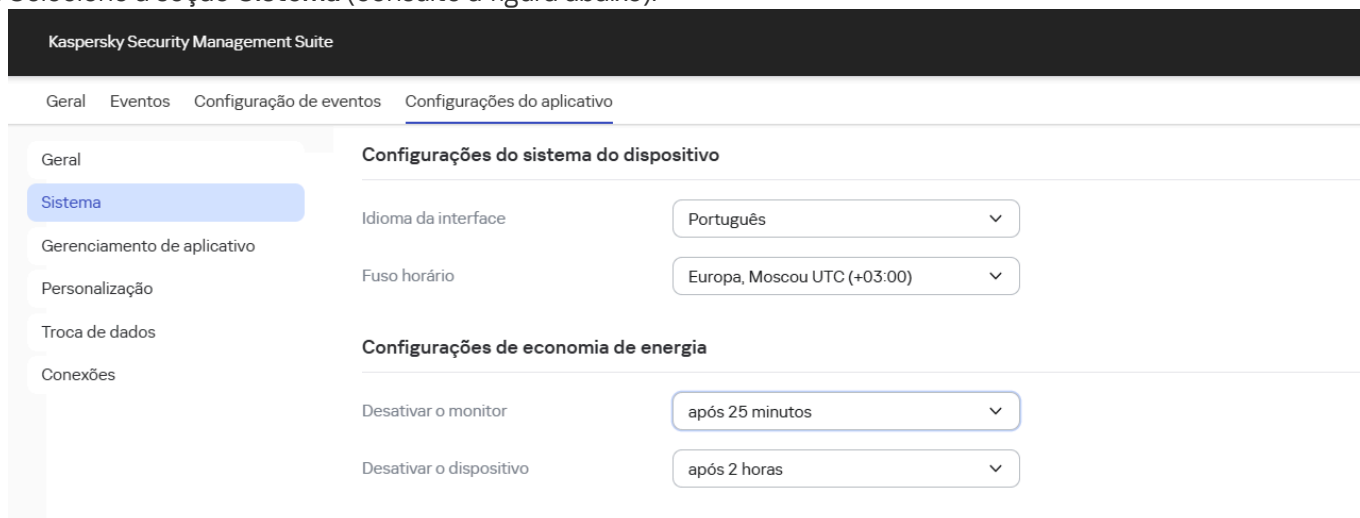
Para definir as configurações sistema do Kaspersky Thin Client pelo Web Console:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.
5. Selecione a guia **Configurações do aplicativo**.

6. Selecione a seção **Sistema** (consulte a figura abaixo).



Janela para definir as configurações de sistema do Kaspersky Thin Client por meio do Web Console

7. No bloco **Configurações do sistema do dispositivo**, selecione os valores relevantes nas listas suspensas **Idioma da interface** e **Fuso horário**.

8. No bloco **Configurações de economia de energia**, defina as seguintes configurações:

- Na lista suspensa **Desativar o monitor**, selecione o período de inatividade do sistema após o qual o monitor será desativado.
- Na lista suspensa **Desativar o dispositivo**, selecione o período de inatividade do sistema após o qual o thin client será desativado.

9. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado em um thin client após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração do encaminhamento de logs do Kaspersky Thin Client para um servidor de log: um dispositivo

No Web Console, é possível alterar o endereço do [servidor de log](#) para o qual os [logs de eventos e auditoria](#) do Kaspersky Thin Client serão encaminhados.

Para configurar o encaminhamento de logs do Kaspersky Thin Client para o servidor de log por meio do Web Console:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.
5. Selecione a guia **Configurações do aplicativo**.
6. Selecione a seção **Troca de dados** (consulte a figura abaixo).

Janela para configurar o encaminhamento de logs do Kaspersky Thin Client por meio do Web Console

7. No campo **Endereço de encaminhamento do log**, insira o endereço do servidor de log de destino no formato `https://<endereço do servidor>`.

Para receber logs de eventos e auditoria do Kaspersky Thin Client, sua organização deve ter um servidor de log implementado que atenda aos [requisitos de hardware and software](#).

8. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado em um thin client após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Personalização do Kaspersky Thin Client: um dispositivo

No Web Console, é possível carregar as imagens e defini-las como plano de fundo da área de trabalho ou da tela de bloqueio do Kaspersky Thin Client instalado. Os seguintes formatos de arquivo são compatíveis: JPEG, PNG e JPG. O tamanho máximo do arquivo é 15 MB. Também é possível excluir as imagens carregadas do Web Console.

Por padrão, um plano de fundo padrão é definido no desktop e na tela de bloqueio do Kaspersky Thin Client. Caso você tenha definido o plano de fundo, será possível redefinir as configurações de personalização para reverter para a imagem padrão.

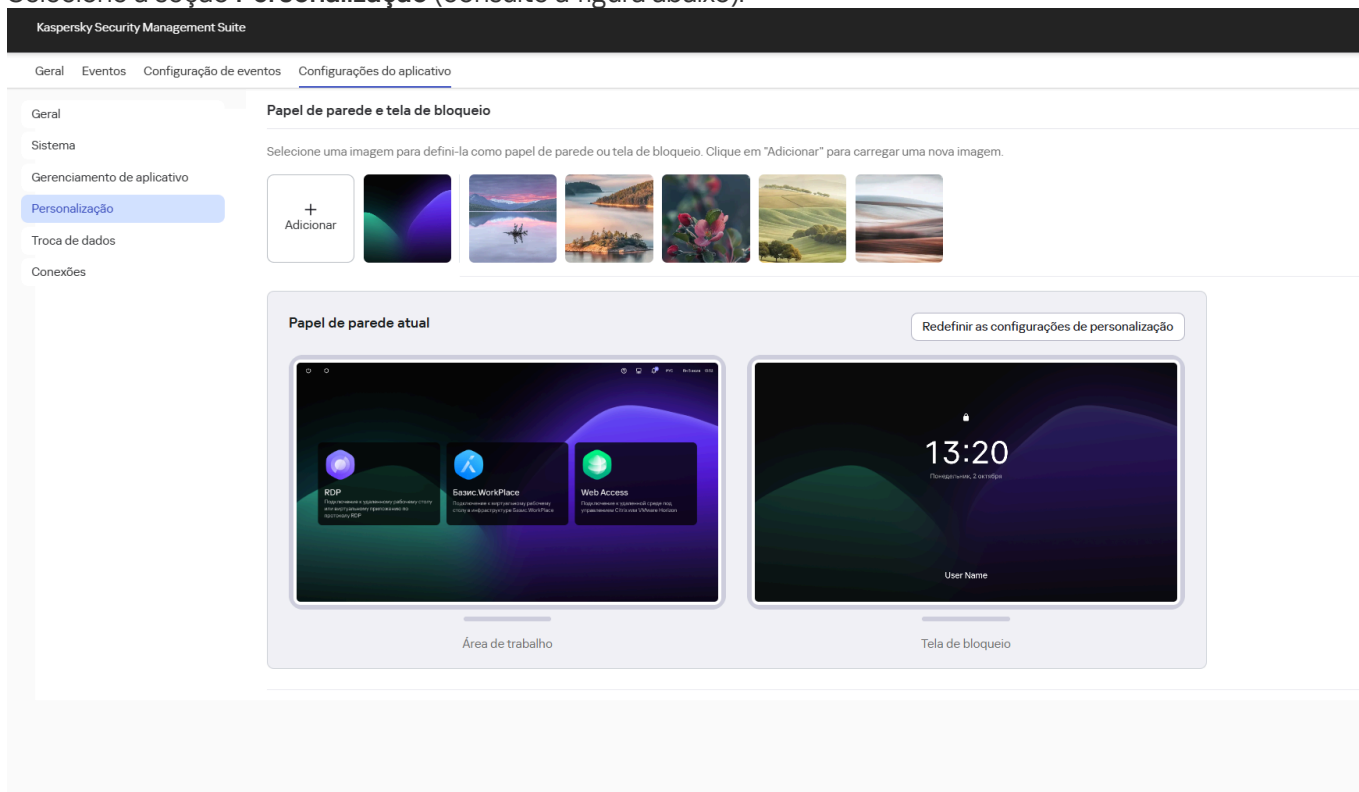
Não é possível alterar o plano de fundo na interface do Kaspersky Thin Client. Em vez disso, é possível alterar o plano de fundo das telas somente pelo Web Console. A imagem definida por meio do Web Console também mudará para o plano de fundo padrão [se a redefinição de fábrica for feita](#).

Para alterar a tela de bloqueio ou o plano de fundo da área de trabalho do Kaspersky Thin Client:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.
5. Selecione a guia **Configurações do aplicativo**.
6. Selecione a seção **Personalização** (consulte a figura abaixo).



Janela para definir as configurações de personalização do Kaspersky Thin Client por meio do Web Console

7. Para alterar o plano de fundo da área de trabalho ou da tela de bloqueio, siga estas etapas:
 - a. Selecione a imagem que deseja definir como plano de fundo.
 - Caso queira carregar uma nova imagem para o Web Console, clique no botão **Adicionar**.
Na janela exibida, arraste a imagem desejada para a área de carregamento ou clique em **Upload a file or drag and drop it here** e selecione a imagem desejada na janela exibida.
 - Caso queira usar uma imagem que já foi carregada no Web Console, clique na miniatura da imagem.

Uma janela de visualização será exibida para o posicionamento da imagem selecionada nas telas do Kaspersky Thin Client.

Caso queira salvar a imagem no Web Console sem defini-la como plano de fundo, vá para a etapa c. destas instruções.

b. Marque as caixas ao lado das telas nas quais deseja definir a imagem como plano de fundo:

- **Área de trabalho:** a imagem será definida como o [plano de fundo da área de trabalho do Kaspersky Thin Client](#).
- **Tela de bloqueio:** a imagem será definida como o [plano de fundo da tela de bloqueio](#).

c. Clique em **Salvar** na janela de visualização.

A tela principal da seção **Personalização** será exibida. O plano de fundo será definido para as telas selecionadas.

8. Para excluir uma imagem carregada no Web Console, passe o mouse sobre a miniatura da imagem e clique no botão  exibido.

Confirme as ações na janela exibida.

A imagem será excluída permanentemente do Web Console. Caso a imagem seja selecionada como plano de fundo em qualquer tela, o plano de fundo padrão será definido em seu lugar.

9. Para reverter todas as telas para o plano de fundo padrão, clique em **Redefinir as configurações de personalização** e confirme as ações na janela exibida.

Um plano de fundo padrão será definido no desktop e na tela de bloqueio do Kaspersky Thin Client.

10. Clique em **Salvar** na parte inferior da seção da janela **Personalização**.

As alterações serão salvas e aplicadas no thin client dentro de uma hora após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Definição das configurações para conexão remota a um thin client usando o Web Console: um dispositivo

No Web Console, é possível definir as seguintes configurações para conexão remota com um thin client:

- **Modo de acesso de gerenciamento remoto:** determina as condições e o procedimento para conexão com o thin client.
- **O modo de acesso à sessão remota em execução no thin client quando a conexão é estabelecida** (doravante também chamado de "tela do ambiente remoto").

Pode ser necessário restringir o acesso à tela do ambiente remoto se o usuário do thin client estiver trabalhando com dados sensíveis ou confidenciais.

Para definir as configurações para conexão remota com um thin client:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.
5. Selecione a guia **Configurações do aplicativo**.
6. Selecione a seção **Troca de dados** (consulte a figura abaixo).

Kaspersky Security Management Suite

Gerar logs

Endereço de encaminhamento do log

Confirmar ações do usuário

Insira o código fornecido pelo usuário na interface do Kaspersky Thin Client, gere um código de confirmação e compartilhe-o com o usuário. O código é válido por 10 minutos.

Código fornecido pelo usuário Gerar código de confirmação

Gerenciamento remoto

Configurar conexão remota com o thin client

Conexão remota

☒ Permitir mediante solicitação

☐ Permitir automaticamente ⓘ

☐ Negar

Acesso à sessão remota

☒ Permitir mediante solicitação

☐ Permitir automaticamente ⓘ

☐ Negar

Dados de conexão do thin client

Endereço IP do dispositivo 10.0.0.0

Senha para conexão remota

Janela para configurar o gerenciamento remoto do thin client pelo Web Console

7. Na seção **Gerenciamento remoto**, selecione o modo de acesso para gerenciamento remoto do thin client:
- **Permitir automaticamente**
- Nesse modo, o administrador poderá se conectar remotamente ao thin client após o usuário [aceitar a solicitação de gerenciamento remoto na interface do Kaspersky Thin Client](#). Caso o usuário rejeite a solicitação, a conexão será encerrada. Caso não haja resposta em 30 segundos, a conexão será estabelecida automaticamente.

- **Permitir mediante solicitação**

Nesse modo, o administrador poderá se conectar remotamente ao thin client somente após o usuário [aceitar a solicitação de gerenciamento remoto na interface do Kaspersky Thin Client](#). Caso o usuário rejeite a solicitação, a conexão será encerrada.

- **Negar**

Nesse modo, o administrador não pode se conectar remotamente ao thin client.

Ao definir o modo **Permitir automaticamente** ou **Permitir mediante solicitação**, o grupo de configurações **Acesso à sessão remota** é desbloqueado.

8. No grupo de configurações **Acesso à sessão remota**, selecione o modo de acesso à tela do ambiente remoto:

- **Permitir automaticamente**

Nesse modo, após se conectar ao thin client, o administrador pode acessar a tela do ambiente remoto sem confirmação do usuário.

- **Permitir mediante solicitação**

Nesse modo, após se conectar ao thin client, o administrador pode acessar a tela do ambiente remoto somente após o usuário [aceitar a solicitação de acesso na interface do Kaspersky Thin Client](#).

- **Negar**

Nesse modo, o administrador não pode gerenciar remotamente o thin client até que o usuário encerre a sessão remota manualmente.

9. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado em um thin client após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração da inicialização automática e exibição de aplicativos: um dispositivo

No Web Console, é possível selecionar um [aplicativo](#) que será iniciado automaticamente após ligar o thin client e inicializar o sistema, e também é possível especificar quais aplicativos serão exibidos no Desktop do Kaspersky Thin Client.

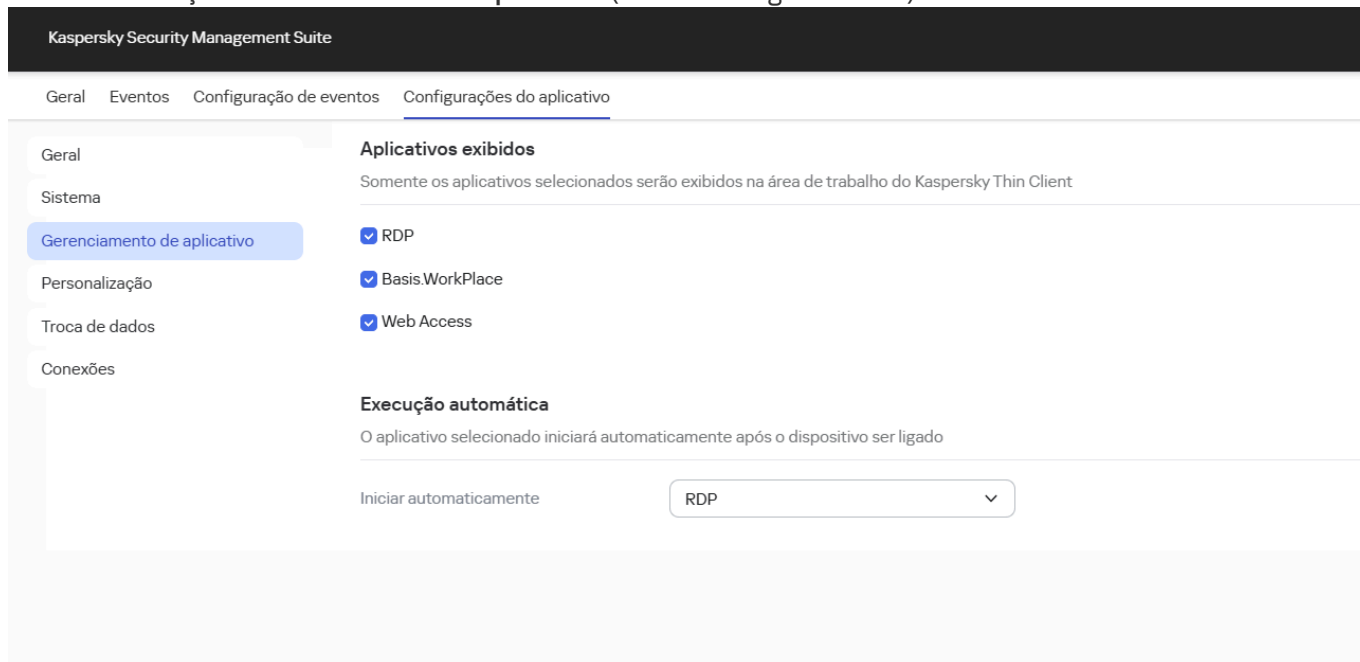
Para configurar a inicialização automática e a exibição de aplicativos:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.

4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.
5. Selecione a guia **Configurações do aplicativo**.
6. Selecione a seção **Gerenciamento de aplicativo** (consulte a figura abaixo).



Janela de configuração para inicialização automática e exibição de aplicativos por meio do Web Console

7. No bloco **Aplicativos exibidos**, marque as caixas de seleção ao lado dos aplicativos que serão exibidos no Desktop do Kaspersky Thin Client.

Na lista suspensa **Iniciar automaticamente**, selecione o aplicativo que será iniciado automaticamente após ligar o dispositivo e inicializar o sistema. Caso selecione **Desativado**, a inicialização automática será desativada.

8. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado em um thin client após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Definição das configurações do Kaspersky Thin Client para um grupo de administração pelo Web Console

No Web Console, é possível usar as [políticas](#) para definir as configurações do Kaspersky Thin Client instalado em thin clients conectados ao Kaspersky Security Center e adicionados a um [grupo de administração](#).

Definição das principais configurações do Kaspersky Thin Client pelo Web Console: grupo de administração

No Web Console, é possível usar [políticas](#) para atribuir nomes a thin clients em um [grupo de administração](#) e especificar os detalhes de contato do administrador. Esses dados serão exibidos na interface do Kaspersky Thin Client desses dispositivos.

Para definir as principais configurações do Kaspersky Thin Client pelo Web Console:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Geral** (consulte a figura abaixo).

The screenshot displays the 'Kaspersky Security Management Suite' interface. At the top, there's a navigation bar with tabs: 'Geral', 'Configuração de eventos', 'Configurações do aplicativo' (which is active), and 'Histórico de revisões'. On the left, a sidebar lists various settings categories: 'Geral' (selected), 'Sistema', 'Gerenciamento de aplicativo', 'Personalização', 'Troca de dados', 'Conexões', and 'Certificados'. The main content area is titled 'Regra de nomeação do grupo de dispositivos'. It includes a description: 'Todos os dispositivos no grupo terão um nome composto. Exemplo: Accounting-00000001-Voronezh.' Below this, there are two input fields: 'Nome' (with a placeholder 'Insira o nome') and 'Sufixo' (with a placeholder 'Insira as informações adicionais'), separated by '- ID do dispositivo -'. Further down, there's a section 'Contatos do Suporte Técnico' with the text 'Os usuários verão os detalhes de contato na interface do Kaspersky Thin Client.' and a 'Detalhes de contato' field with a placeholder: 'Especifique o número de telefone e o endereço de e-mail do suporte técnico ou do administrador do sistema da sua empresa'.

Janela para definir as principais configurações do Kaspersky Thin Client instalado em thin clientes em um grupo de administração por meio do Web Console

5. Defina as configurações necessárias:

- Na seção **Regra de nomeação do grupo de dispositivos**, insira o nome e informações adicionais nos campos relevantes. Esses dados são exibidos no nome de cada thin client adicionado ao grupo de administração. É possível inserir letras maiúsculas e minúsculas do alfabeto cirílico ou latino, além de caracteres especiais. Comprimento máximo do texto em cada campo: 10 caracteres.

Os nomes dos thin clients também incluem um identificador (ID). Trata-se de um conjunto exclusivo de oito caracteres gerado de forma automática para cada dispositivo adicionado ao grupo de administração. É possível [alterar o identificador de um thin client individual](#).

- Na seção **Contatos do Suporte Técnico**, no campo **Detalhes de contato**, insira o número de telefone e o nome do administrador, ou, por exemplo, o endereço de e-mail de seu serviço de suporte técnico. O número de caracteres nesse campo não deve exceder 80 caracteres.

As informações inseridas serão exibidas para thin clients adicionados ao grupo de administração na interface do Kaspersky Thin Client: no painel de controle, nas janelas para confirmar uma [redefinição das configurações e dados do Kaspersky Thin Client](#) e as [alterações nas configurações de conexão do Kaspersky Security Center](#), e quando [o certificado para a conexão com o Kaspersky Security Center for substituído](#).

6. Se você quiser que as configurações definidas sejam aplicadas ao Kaspersky Thin Client instalado nos grupos de administração secundários, e se não quiser que elas estejam disponíveis para edição no Kaspersky Thin Client no grupo de administração atual, mude os [botões de alternância ao lado dos blocos pertinentes de configurações](#) para a posição **Aplicado**.

7. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado nos thin clients adicionados ao grupo de administração após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

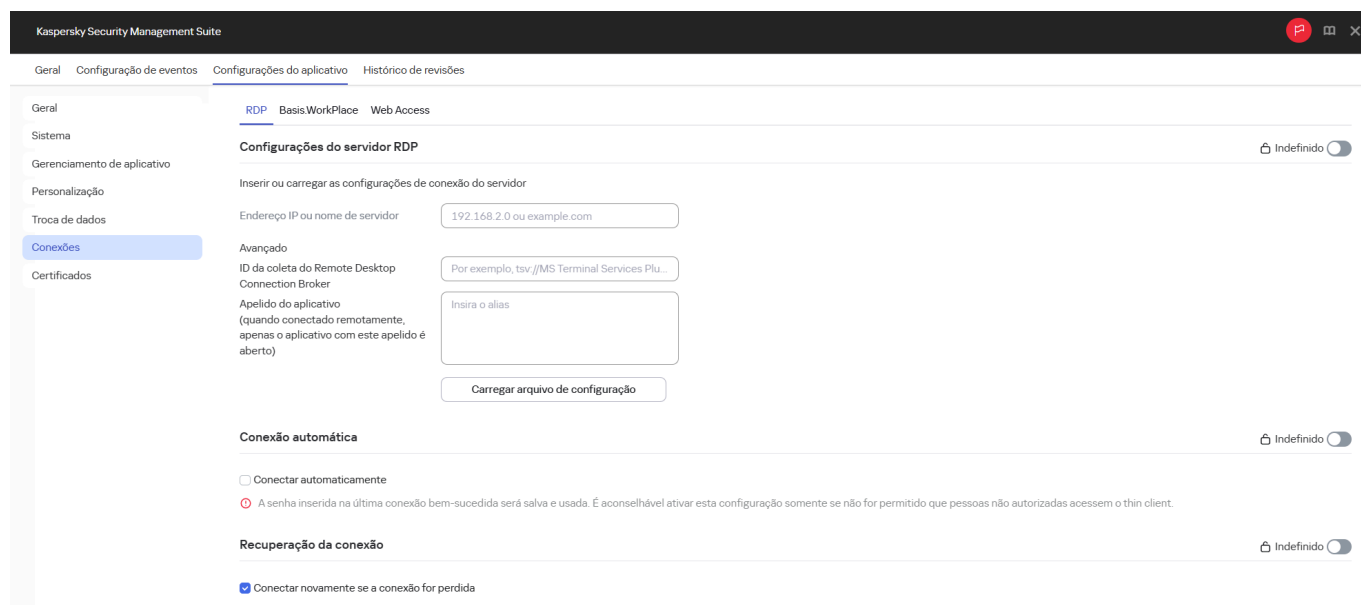
Configuração de uma conexão com um ambiente remoto por meio do aplicativo RDP pelo Web Console: grupo de administração

No Web Console, é possível usar [políticas](#) para definir as configurações da [conexão a um ambiente remoto pelo aplicativo RDP](#).

Para definir as configurações para a conexão com um ambiente remoto pelo aplicativo RDP:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.
4. Selecione **Conexões** → **RDP**.

Isso abre uma janela na qual é possível definir as configurações para conexão com um ambiente remoto (veja a figura abaixo).



The screenshot shows the 'Configurações do servidor RDP' (RDP Server Settings) page in the Kaspersky Security Management Suite Web Console. The page is divided into several sections:

- Configurações do servidor RDP**: This section includes a toggle for 'Indefinido' (Undefined) and a text input field for 'Endereço IP ou nome de servidor' (IP address or server name) with the value '192.168.2.0 ou example.com'.
- Avançado**: This section includes a text input field for 'ID da coleta do Remote Desktop Connection Broker' (Advanced ID of the Remote Desktop Connection Broker collection) with the value 'Por exemplo, tsv://MS Terminal Services Plu...'. Below this is a text input field for 'Apelido do aplicativo' (Application alias) with the value 'Insira o alias'.
- Conexão automática**: This section includes a checkbox for 'Conectar automaticamente' (Connect automatically) and a note: 'A senha inserida na última conexão bem-sucedida será salva e usada. É aconselhável ativar esta configuração somente se não for permitido que pessoas não autorizadas acessem o thin client.' (The password entered in the last successful connection will be saved and used. It is recommended to activate this configuration only if it is not permitted for unauthorized persons to access the thin client.)
- Recuperação da conexão**: This section includes a checkbox for 'Conectar novamente se a conexão for perdida' (Connect again if the connection is lost).

Janela de configuração para se conectar com um ambiente remoto no aplicativo RDP pelo Web Console: grupo de administração

5. No campo **Endereço IP ou nome de servidor**, insira o endereço IP ou o nome do servidor para fazer a conexão com um ambiente remoto por meio do RDP.
6. Caso precise usar o Microsoft Remote Desktop Connection Broker para conexão com um desktop remoto, use o campo **ID da coleta do Remote Desktop Connection Broker** para especificar o ID da coleção no formato `tsv://MS Terminal Services Plugin.1.collection_id` (`collection_id` refere-se ao identificador específico da coleção).

Caso precise iniciar um aplicativo virtual, especifique o apelido do aplicativo no campo **Apelido do aplicativo**.

Caso tenha um arquivo de configuração contendo as configurações para se conectar com o Microsoft Remote Desktop Connection Broker e, caso seja necessário, o nome do aplicativo a ser aberto, carregue o arquivo clicando em **Carregar arquivo de configuração**. Neste caso, não é necessário preencher os campos **ID da coleta do Remote Desktop Connection Broker** e **Apelido do aplicativo**.

7. Caso queira restaurar automaticamente uma conexão do desktop remoto que foi desconectada inesperadamente, marque a caixa de seleção **Conectar novamente se a conexão for perdida**.
8. No bloco de configurações **Redirecionamento de dispositivos**, selecione os dispositivos a serem redirecionados para o ambiente remoto: **Cartões inteligentes, Unidades USB, Impressoras e outros dispositivos, Microfone, Dispositivos de reprodução de áudio, Câmera da Web (vídeo) e Scanner**. O volume do áudio e outras configurações são gerenciados no ambiente remoto.

Para redirecionar corretamente os dispositivos USB para um desktop remoto usando o sistema operacional Windows 10, é preciso ativar o Microsoft Remote Desktop Services e permitir o redirecionamento de dispositivos Plug and Play nas configurações do Remote Desktop Services. Para o Microsoft Windows Server 2016 e 2019, é necessário ativar as conexões remotas por meio dos Serviços de Desktop Remoto e permitir a configuração das regras de gerenciamento remoto nesses serviços.

9. No bloco **Qualidade da imagem**, marque as caixas de seleção ao lado das configurações gráficas do desktop remoto que deseja usar: **Fontes suaves**, **Animação do menu**, **Plano de fundo**, **Mostrar o conteúdo das janelas ao arrastar** e **Tema aprimorado**.

Ativar as configurações de exibição do desktop remoto remota poderá afetar a velocidade das operações do Kaspersky Thin Client.

10. Caso dois monitores estejam instalados em sua estação de trabalho e o usuário quiser que uma imagem do desktop remoto seja exibida em ambos os monitores, marque a caixa de seleção **Usar dois monitores** no bloco **Gerenciamento de monitores**.
11. Para melhorar o desempenho quando conectado com desktops remotos ou aplicativos, no bloco **Desempenho**, marque **Melhorar o desempenho gráfico**.
12. Para se conectar a um desktop remoto ou aplicativo virtual automaticamente quando o aplicativo RDP for iniciado, no bloco **Conexão automática**, marque a caixa de seleção **Conectar automaticamente**.
- Para ativar a função, o usuário deve se conectar e se desconectar manualmente do ambiente remoto uma vez. Ao fazer isso, os seguintes dados para a conexão com o servidor RDP serão salvos no armazenamento do thin client: nome de usuário, endereço do servidor e senha. Na próxima vez que o aplicativo RDP for iniciado, essas credenciais serão usadas para iniciar automaticamente uma conexão ao ambiente remoto. Caso a função de conexão automática seja desativada, a senha salva será excluída do armazenamento do dispositivo.
- O Web Console não permite definir uma senha para se conectar com um ambiente remoto.
- Para se conectar automaticamente ao ambiente remoto no aplicativo RDP imediatamente após a inicialização do Kaspersky Thin Client, [configure a inicialização automática do aplicativo](#).
13. Se você quiser que as configurações definidas sejam aplicadas ao Kaspersky Thin Client instalado nos grupos de administração secundários, e se não quiser que elas estejam disponíveis para edição no Kaspersky Thin Client no grupo de administração atual, mude os [botões de alternância ao lado dos blocos pertinentes de configurações](#) para a posição **Aplicado**.
14. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado nos thin clients adicionados ao grupo de administração após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração de uma conexão com um ambiente remoto usando o aplicativo Basis.WorkPlace pelo Web Console: grupo de administração

No Web Console, é possível usar [políticas](#) para definir as configurações da [conexão a um ambiente remoto implementado na infraestrutura do Basis.WorkPlace](#).

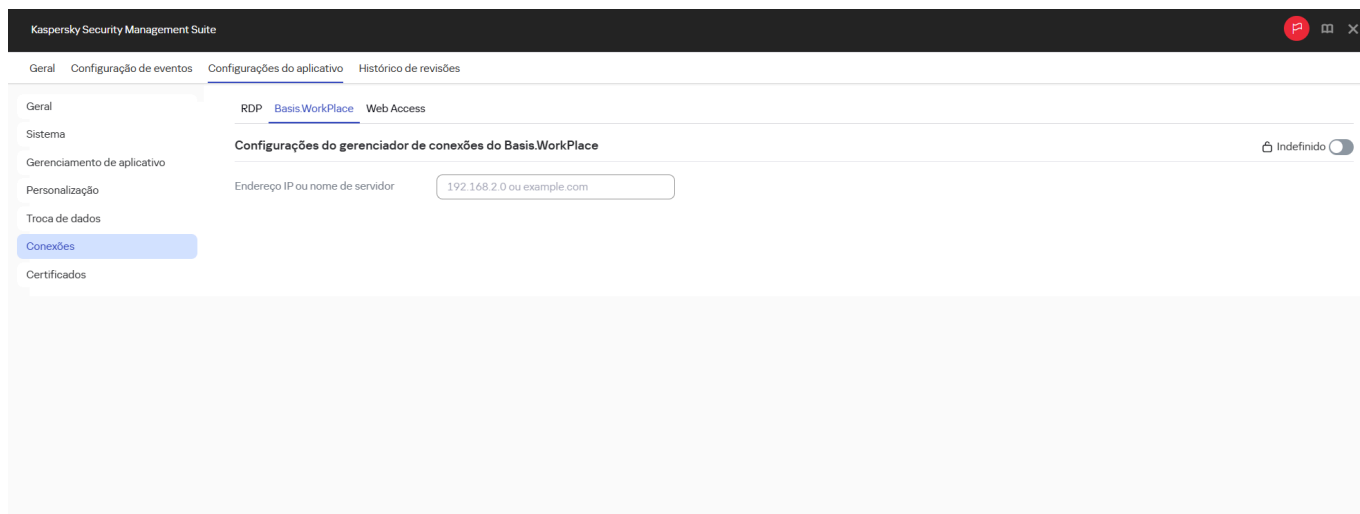
Os usuários não podem iniciar uma alteração de senha no Kaspersky Thin Client.

Para definir as configurações de conexão com um ambiente remoto usando a infraestrutura Basis.WorkPlace:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.

4. Selecione **Conexões** → **Basis.WorkPlace**.

Isso abre uma janela na qual é possível definir as configurações para conexão com um ambiente remoto (veja a figura abaixo).



Janela de configuração para a conexão com um ambiente remoto implementado na infraestrutura do Basis.WorkPlace por meio do Web Console: grupo de administração

5. Em **Endereço IP ou nome de servidor**, insira o endereço IP ou o nome do servidor ao qual se conectar.

6. Se você quiser que as configurações definidas sejam aplicadas ao Kaspersky Thin Client instalado nos grupos de administração secundários, e se não quiser que elas estejam disponíveis para edição no Kaspersky Thin Client no grupo de administração atual, mude os [botões de alternância ao lado dos blocos pertinentes de configurações](#) para a posição **Aplicado**.

7. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado nos thin clients adicionados ao grupo de administração após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração de uma conexão com um ambiente remoto no aplicativo Web Access pelo Web Console: grupo de administração

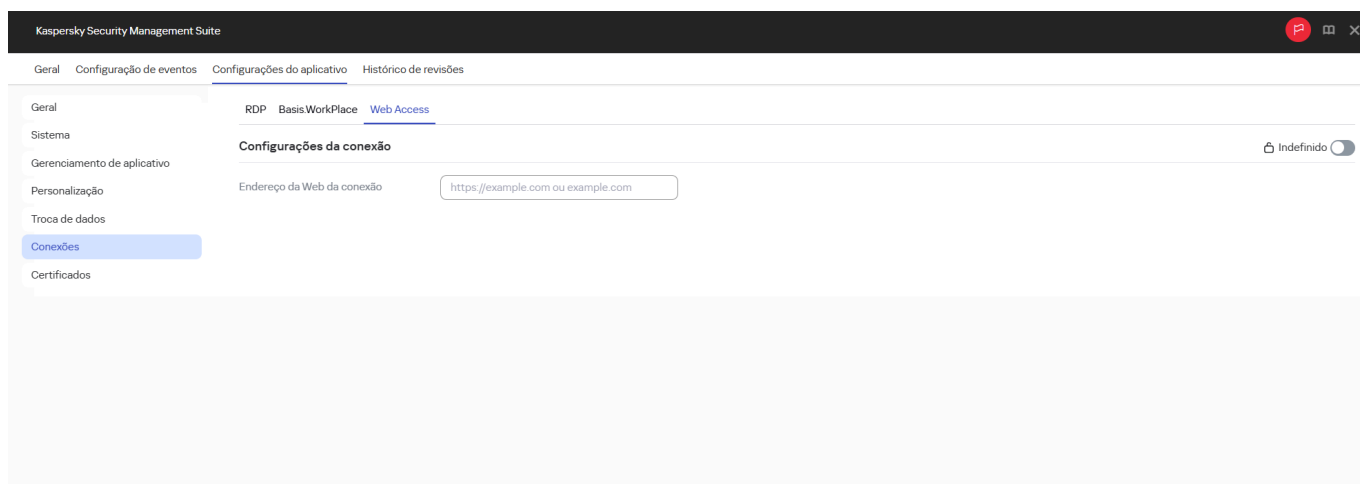
No Web Console, é possível usar [políticas](#) para definir as configurações da [conexão a um ambiente remoto pelo aplicativo Web Access](#).

É possível usar o aplicativo Web Access para se conectar a um ambiente remoto implementado nas infraestruturas do Citrix Workspace. O Web Access é compatível com HTML5 e fornece uma conexão HTTPS segura ao conectar.

Para definir as configurações para a conexão com um ambiente remoto pelo aplicativo Web Access:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.
4. Selecione **Conexões** → **Web Access**.

Isso abre uma janela na qual é possível definir as configurações para conexão com um ambiente remoto (veja a figura abaixo).



Janela de configuração para a conexão com um ambiente remoto usando o aplicativo Web Access pelo Web Console: grupo de administração

5. No campo **Endereço da Web da conexão**, insira o endereço da Web do servidor para se conectar ao ambiente remoto pertinente.
6. Se você quiser que as configurações definidas sejam aplicadas ao Kaspersky Thin Client instalado nos grupos de administração secundários, e se não quiser que elas estejam disponíveis para edição no Kaspersky Thin Client no grupo de administração atual, mude os [botões de alternância ao lado dos blocos pertinentes de configurações](#) para a posição **Aplicado**.
7. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado nos thin clients adicionados ao grupo de administração após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração de monitores e telas pelo Web Console: grupo de administração

No Web Console, é possível usar [políticas](#) para configurar os monitores conectados a thin clients e as configurações das telas do Kaspersky Thin Client.

O Kaspersky Thin Client é compatível com a conexão de dois monitores. O sistema considera um dos monitores como o principal e o outro como secundário. Durante uma [sessão remota](#), o painel de conexão é exibido na tela do monitor principal. A tela do monitor secundário estende ou duplica a imagem do monitor principal. No Web Console, é possível selecionar qual monitor deve ser considerado o monitor principal (doravante também "alterar o layout do monitor").

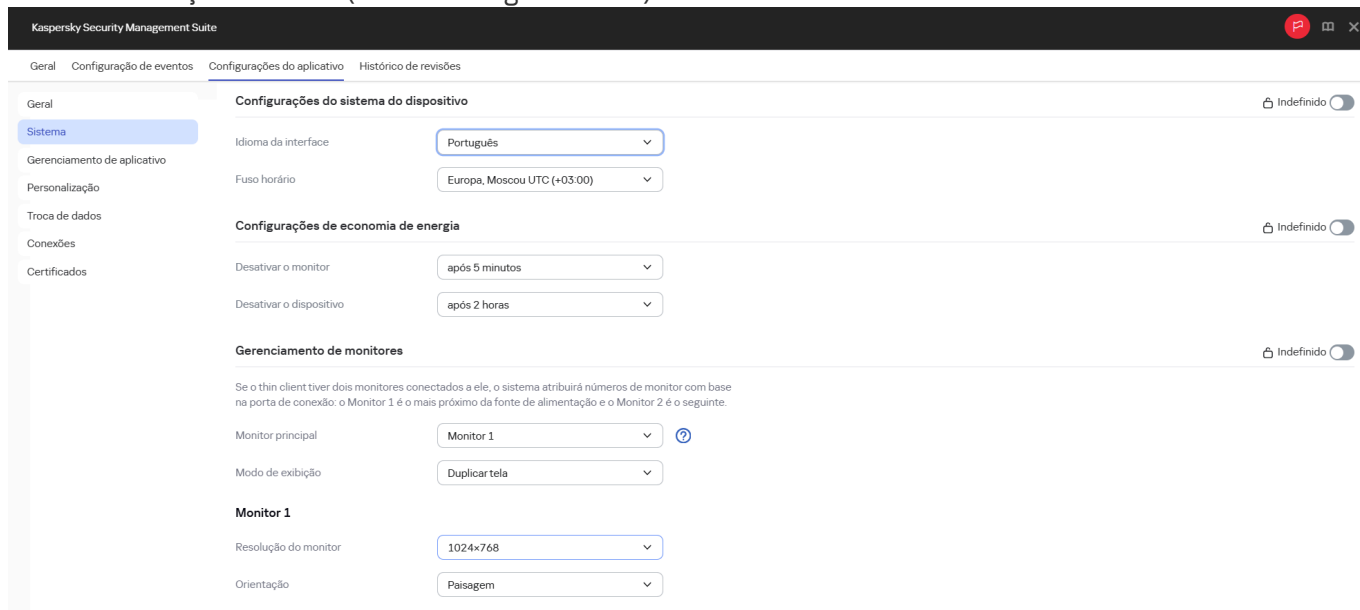
Os monitores são numerados na interface do Web Console. O sistema determina os números dos monitores com base na porta de conexão: o monitor 1 é aquele mais próximo da fonte de alimentação e o monitor 2 é o próximo. Consulte a documentação do fabricante do dispositivo para saber a localização das portas nos [modelos de thin client compatíveis](#).

O Web Console não exibe informações sobre quantos monitores estão conectados a um thin client específico.

Se você quiser que a tela da sessão remota seja exibida em ambos os monitores, ative essa opção nas configurações de conexão do ambiente remoto nos aplicativos [RDP](#) ou [Basis.WorkPlace](#).

Para configurar monitores e telas pelo Web Console:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Sistema** (consulte a figura abaixo).



Janela de configuração de monitores e telas pelo Web Console: grupo de administração

5. No grupo **Gerenciamento de monitores**, defina as configurações necessárias:

- Na lista suspensa **Monitor principal**, selecione qual deve ser considerado o monitor principal.

Se apenas um monitor estiver conectado a um dos thin clients no grupo de administração, as configurações do monitor definido como principal no Web Console serão aplicadas a ele.

- Na lista suspensa **Modo de exibição**, selecione a opção de exibição de imagem:
 - **Estender tela**: a imagem se estenderá por dois monitores.
 - **Duplicar tela**: a imagem da tela do monitor principal será duplicada no monitor secundário.
- Na lista suspensa **Resolução do monitor**, selecione a resolução desejada para a tela selecionada. As resoluções compatíveis serão listadas na seção de requisitos de hardware e software.

Se o valor **Máxima possível** for selecionado, o valor mais alto do parâmetro compatível com o monitor e com o Kaspersky Thin Client será definido.

- Na lista suspensa **Orientação**, selecione a posição da tela:
 - **Paisagem**: a posição padrão da tela.
 - **Paisagem invertida**: a tela gira 180°.

- **Retrato:** a tela gira 90°.
- **Retrato invertido:** a tela gira 270°.

6. Se você quiser que as configurações definidas sejam aplicadas ao Kaspersky Thin Client instalado nos grupos de administração secundários, e se não quiser que elas estejam disponíveis para edição no Kaspersky Thin Client no grupo de administração atual, mude os [botões de alternância ao lado dos blocos pertinentes de configurações](#) para a posição **Aplicado**.

7. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado nos thin clients adicionados ao grupo de administração após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

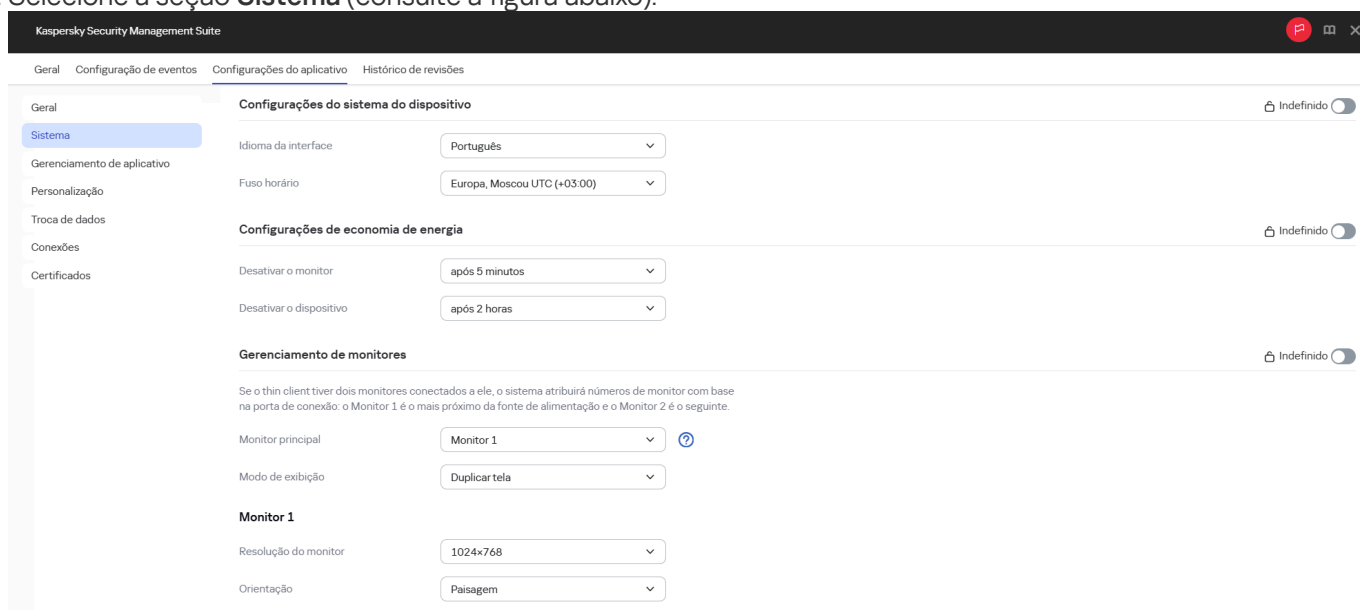
Definição das configurações do Kaspersky Thin Client pelo Web Console: grupo de administração

No Web Console, é possível usar [políticas](#) para configurar o idioma da interface e o fuso horário do Kaspersky Thin Client, além de configurar o horário de desligamento para thin clients e seus monitores respectivos.

O Kaspersky Thin Client 2.3 é compatível com os seguintes idiomas de interface: russo, inglês (EUA), espanhol (México) e português (Brasil).

Para definir as configurações sistema do Kaspersky Thin Client pelo Web Console:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Sistema** (consulte a figura abaixo).



Janela para definir as configurações do sistema pelo Web Console: grupo de administração

5. No bloco **Configurações do sistema do dispositivo**, selecione os valores relevantes nas listas suspensas **Idioma da interface** e **Fuso horário**.

6. No bloco **Configurações de economia de energia**, defina as seguintes configurações:

- Na lista suspensa **Desativar o monitor**, selecione o período de inatividade do sistema após o qual o monitor será desativado.
- Na lista suspensa **Desativar o dispositivo**, selecione o período de inatividade do sistema após o qual o thin client será desativado.

7. Se você quiser que as configurações definidas sejam aplicadas ao Kaspersky Thin Client instalado nos grupos de administração secundários, e se não quiser que elas estejam disponíveis para edição no Kaspersky Thin Client no grupo de administração atual, mude os [botões de alternância ao lado dos blocos pertinentes de configurações](#) para a posição **Aplicado**.

8. Clique em **Salvar** na parte inferior da janela.

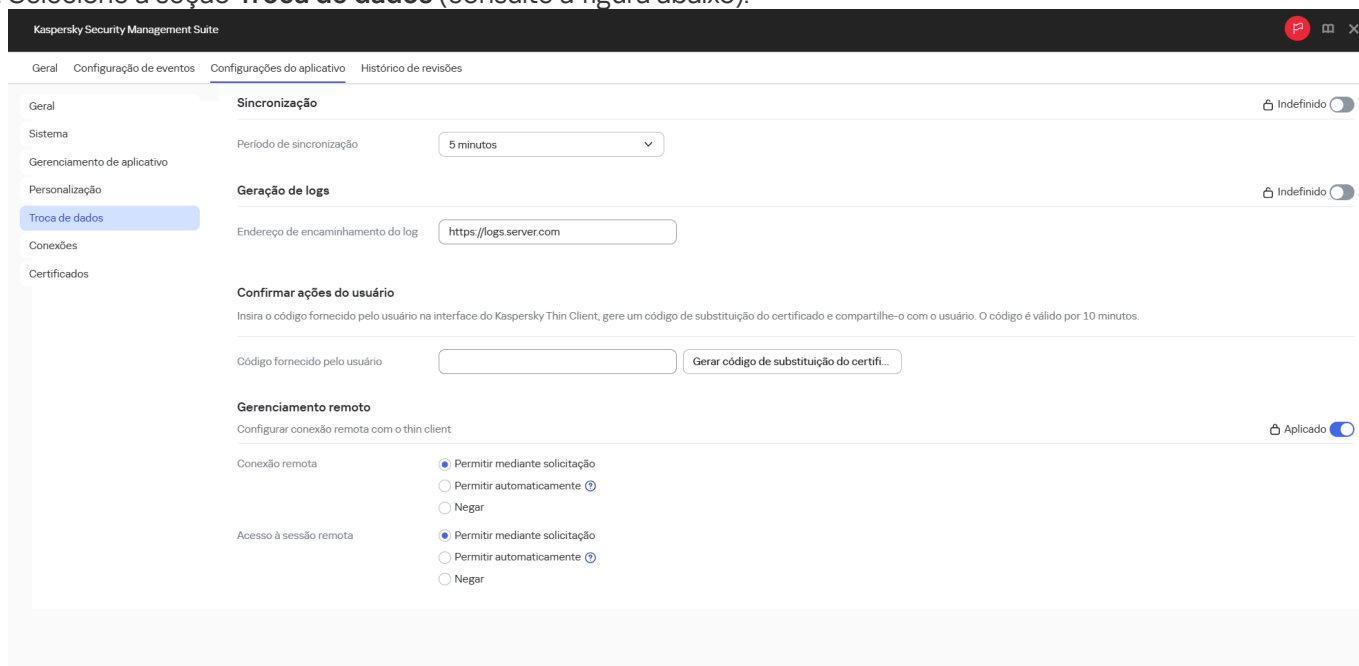
As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado nos thin clients adicionados ao grupo de administração após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração do encaminhamento de logs do Kaspersky Thin Client para um servidor de log: grupo de administração

No Web Console, é possível usar [políticas](#) para alterar o endereço do [servidor de log](#) para o qual os [logs de eventos e auditoria](#) do Kaspersky Thin Client serão encaminhados.

Para configurar o encaminhamento de logs de evento e auditoria para um servidor de log por meio do Web Console:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Troca de dados** (consulte a figura abaixo).



Janela para configurar o encaminhamento de logs do Kaspersky Thin Client por meio do Web Console: grupo de administração

5. No campo **Endereço de encaminhamento do log**, insira o endereço do servidor de log de destino no formato `https://<endereço do servidor>`.

Para receber logs de eventos e auditoria do Kaspersky Thin Client, sua organização deve ter um servidor de log implementado que atenda aos [requisitos de hardware and software](#).

6. Se você quiser que as configurações definidas sejam aplicadas ao Kaspersky Thin Client instalado nos grupos de administração secundários, e se não quiser que elas estejam disponíveis para edição no Kaspersky Thin Client no grupo de administração atual, mude os [botões de alternância ao lado dos blocos pertinentes de configurações](#) para a posição **Aplicado**.
7. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado nos thin clients adicionados ao grupo de administração após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Personalização do Kaspersky Thin Client: grupo de administração

No Web Console, é possível usar [políticas](#)  carregar as imagens e defini-las como plano de fundo da área de trabalho ou da tela de bloqueio do Kaspersky Thin Client instalado. Os seguintes formatos de arquivo são compatíveis: JPEG, PNG e JPG. O tamanho máximo do arquivo é 15 MB. Também é possível excluir as imagens carregadas do Web Console.

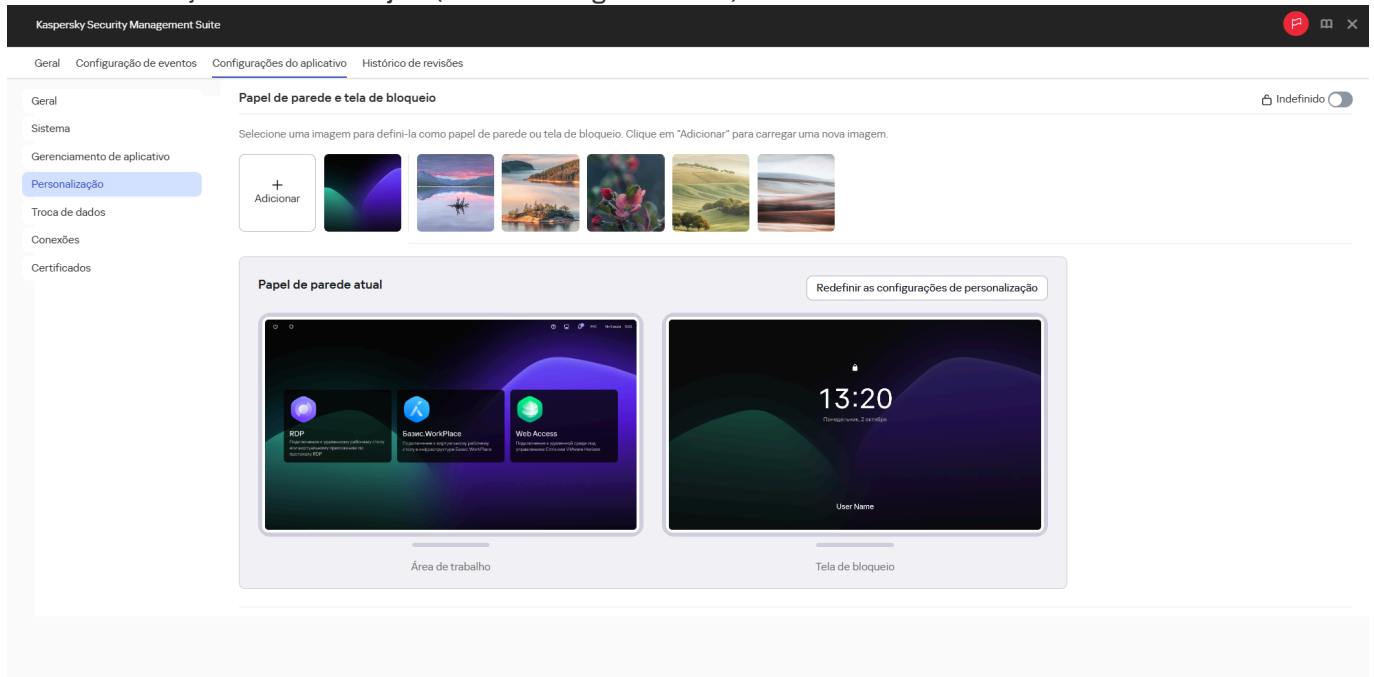
Por padrão, um plano de fundo padrão é definido no desktop e na tela de bloqueio do Kaspersky Thin Client. Caso você tenha definido o plano de fundo, será possível redefinir as configurações de personalização para reverter para a imagem padrão.

Não é possível alterar o plano de fundo na interface do Kaspersky Thin Client. Em vez disso, é possível alterar o plano de fundo das telas somente pelo Web Console. A imagem definida por meio do Web Console também mudará para o plano de fundo padrão [se a redefinição de fábrica for feita](#).

Para alterar a tela de bloqueio ou o plano de fundo da área de trabalho do Kaspersky Thin Client pelo Web Console:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.

4. Selecione a seção **Personalização** (consulte a figura abaixo).



Janela para definir as configurações de personalização do Kaspersky Thin Client por meio do Web Console: grupo de administração

5. Para alterar o plano de fundo da área de trabalho ou da tela de bloqueio, siga estas etapas:

a. Selecione a imagem que deseja definir como plano de fundo.

- Caso queira carregar uma nova imagem para o Web Console, clique no botão **Adicionar**.
Na janela exibida, arraste a imagem desejada para a área de carregamento ou clique em **Upload a file or drag and drop it here** e selecione a imagem desejada na janela exibida.
- Caso queira usar uma imagem que já foi carregada no Web Console, clique na miniatura da imagem.

Uma janela de visualização será exibida para o posicionamento da imagem selecionada nas telas do Kaspersky Thin Client.

Caso queira salvar a imagem no Web Console sem defini-la como plano de fundo, vá para a etapa c. destas instruções.

b. Marque as caixas ao lado das telas nas quais deseja definir a imagem como plano de fundo:

- **Área de trabalho:** a imagem será definida como o [plano de fundo da área de trabalho do Kaspersky Thin Client](#).
- **Tela de bloqueio:** a imagem será definida como o [plano de fundo da tela de bloqueio](#).

c. Clique em **Salvar** na janela de visualização.

A tela principal da seção **Personalização** será exibida. O plano de fundo será definido para as telas selecionadas.

6. Para excluir uma imagem carregada no Web Console, passe o mouse sobre a miniatura da imagem e clique no botão **X** exibido.

Confirme as ações na janela exibida.

A imagem será excluída permanentemente do Web Console. Caso a imagem seja selecionada como plano de fundo em qualquer tela, o plano de fundo padrão será definido em seu lugar.

7. Para reverter todas as telas para o plano de fundo padrão, clique em **Redefinir as configurações de personalização** e confirme as ações na janela exibida.

8. Um plano de fundo padrão será definido no desktop e na tela de bloqueio do Kaspersky Thin Client.

9. Se você quiser que as configurações definidas sejam aplicadas ao Kaspersky Thin Client instalado nos grupos de administração secundários, e se não quiser que elas estejam disponíveis para edição no Kaspersky Thin Client no grupo de administração atual, mude os [botões de alternância ao lado dos blocos pertinentes de configurações](#) para a posição **Aplicado**.

10. Clique em **Salvar** na parte inferior da seção da janela **Personalização**.

As alterações serão salvas e aplicadas aos thin clients adicionados ao grupo de administração dentro de uma hora após a sincronização do Kaspersky Security Center com o Kaspersky Thin Client.

Definição das configurações para conexão remota com um thin client usando o Web Console: grupo de administração

No Web Console, é possível usar [políticas](#) para definir as seguintes configurações de conexão remota:

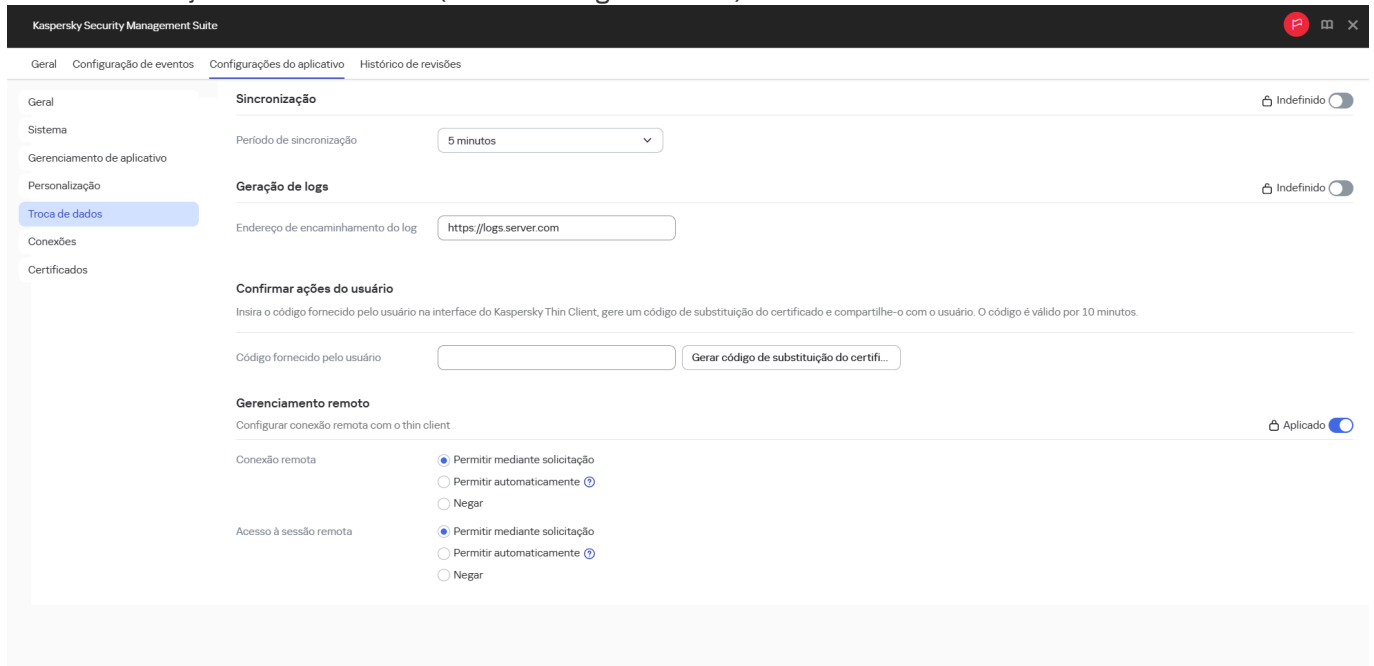
- Modo de acesso de gerenciamento remoto: determina as condições e o procedimento para conexão com o thin client.
- O modo de acesso à sessão remota em execução no thin client quando a conexão é estabelecida (doravante também chamado de "tela do ambiente remoto").

Pode ser necessário restringir o acesso à tela do ambiente remoto se o usuário do thin client estiver trabalhando com dados sensíveis ou confidenciais.

Para definir as configurações para conexão remota com um thin client:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.

4. Selecione a seção **Troca de dados** (consulte a figura abaixo).



Janela para configurar uma conexão remota com um thin client pelo Web Console: grupo de administração

5. Na seção **Gerenciamento remoto**, selecione o modo de acesso para gerenciamento remoto do thin client:

- **Permitir automaticamente**

Nesse modo, o administrador poderá se conectar remotamente ao thin client após o usuário [aceitar a solicitação de gerenciamento remoto na interface do Kaspersky Thin Client](#). Caso o usuário rejeite a solicitação, a conexão será encerrada. Caso não haja resposta em 30 segundos, a conexão será estabelecida automaticamente.

- **Permitir mediante solicitação**

Nesse modo, o administrador poderá se conectar remotamente ao thin client somente após o usuário [aceitar a solicitação de gerenciamento remoto na interface do Kaspersky Thin Client](#). Caso o usuário rejeite a solicitação, a conexão será encerrada.

- **Negar**

Nesse modo, o administrador não pode se conectar remotamente ao thin client.

Ao definir o modo **Permitir automaticamente** ou **Permitir mediante solicitação**, o grupo de configurações **Acesso à sessão remota** é desbloqueado.

6. No grupo de configurações **Acesso à sessão remota**, selecione o modo de acesso à tela do ambiente remoto:

- **Permitir automaticamente**

Nesse modo, após se conectar ao thin client, o administrador pode acessar a tela do ambiente remoto sem confirmação do usuário.

- **Permitir mediante solicitação**

Nesse modo, após se conectar ao thin client, o administrador pode acessar a tela do ambiente remoto somente após o usuário [aceitar a solicitação de acesso na interface do Kaspersky Thin Client](#).

- **Negar**

Nesse modo, o administrador não pode gerenciar remotamente o thin client até que o usuário encerre a sessão remota manualmente.

7. Se você quiser que as configurações definidas sejam aplicadas ao Kaspersky Thin Client instalado nos grupos de administração secundários, e se não quiser que elas estejam disponíveis para edição no Kaspersky Thin Client no grupo de administração atual, mude os [botões de alternância ao lado dos blocos pertinentes de configurações](#) para a posição **Aplicado**.

8. Clique em **Salvar** na parte inferior da janela.

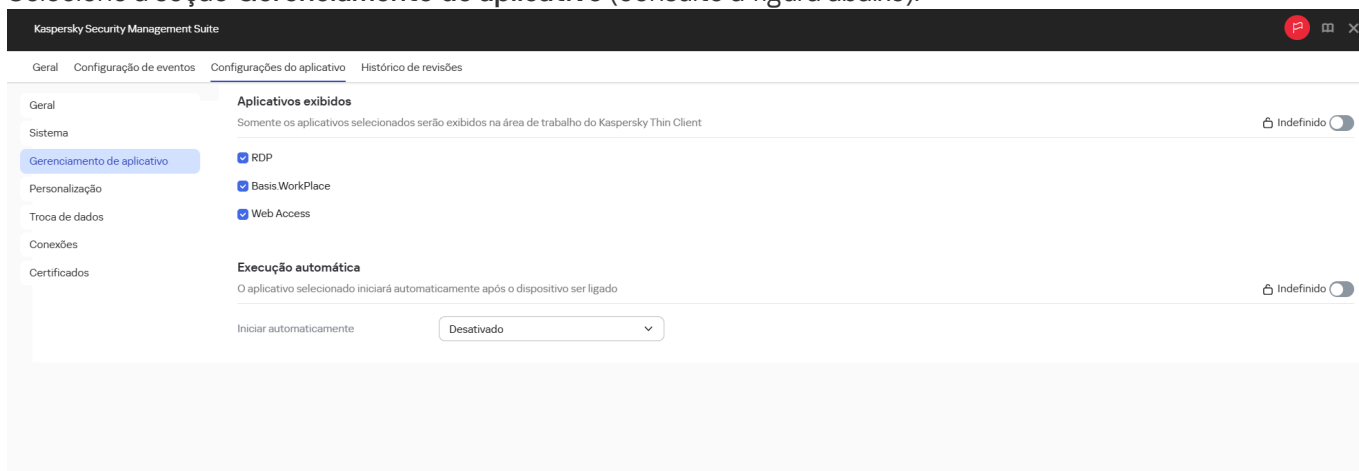
As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado nos thin clients adicionados ao grupo de administração após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Configuração da inicialização automática e exibição de aplicativos: grupo de administração

No Web Console, é possível usar [políticas](#) ² selecionar um [aplicativo](#) que será iniciado automaticamente após iniciar o dispositivo e inicializar o sistema, e também é possível especificar quais aplicativos serão exibidos no Desktop do Kaspersky Thin Client.

Para configurar a inicialização automática e a exibição de aplicativos:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Gerenciamento de aplicativo** (consulte a figura abaixo).



Janela de configuração para inicialização automática e exibição de aplicativos por meio do Web Console: grupo de administração

5. No bloco **Aplicativos exibidos**, marque as caixas de seleção ao lado dos aplicativos que serão exibidos no Desktop do Kaspersky Thin Client.

Na lista suspensa **Iniciar automaticamente**, selecione o aplicativo que será iniciado automaticamente após ligar o dispositivo e inicializar o sistema. Caso selecione **Desativado**, a inicialização automática será desativada.

- As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado nos thin clients adicionados ao grupo de administração após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

6. Se você quiser que as configurações definidas sejam aplicadas ao Kaspersky Thin Client instalado nos grupos de administração secundários, e se não quiser que elas estejam disponíveis para edição no Kaspersky Thin Client no grupo de administração atual, mude os [botões de alternância ao lado dos blocos pertinentes de configurações](#) para a posição **Aplicado**.

7. Clique em **Salvar** na parte inferior da janela.

As alterações serão salvas e aplicadas ao Kaspersky Thin Client instalado nos thin clients adicionados ao grupo de administração após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Confirmação das ações do usuário do Kaspersky Thin Client

As seguintes ações do usuário requerem a confirmação do administrador do Kaspersky Security Center:

- [alteração das configurações para conexão com o Kaspersky Security Center](#)
- [alteração de certificados para conexão com o Kaspersky Security Center](#)
- [redefinição de todas as configurações e dados de um thin client](#)

Se um thin client executando o Kaspersky Thin Client não estiver conectado ao Kaspersky Security Center ou estiver conectado, mas não incluído em um [grupo de administração](#), o thin client não enviará solicitações ao administrador para confirmar as ações listadas acima. [Adicione o thin client ao grupo de administração](#) para receber solicitações para confirmar as ações do usuário.

Para confirmar a alteração das configurações para conexão com o Kaspersky Security Center ou redefinir as configurações do Kaspersky Thin Client:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Dispositivos gerenciados**.
2. Na lista exibida, clique no nome pertinente do thin client. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#). Caso o nome do thin client não esteja na lista, [adicione-o a um grupo de administração](#).

Caso uma configuração que esteja sendo definida esteja bloqueada [em uma política criada para um grupo de administração](#), não será possível alterá-la ao configurar o dispositivo individual. [Altere](#) ou [desbloqueie](#) essa configuração na política.

3. Na janela aberta, selecione a guia **Aplicativos**.
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.
Uma janela contendo informações sobre o Kaspersky Thin Client será aberta.
5. Selecione a guia **Configurações do aplicativo**.
6. Selecione a seção **Troca de dados**.

7. No bloco **Confirmar ações do usuário**, insira o código da interface do Kaspersky Thin Client que o usuário lhe enviou e clique em **Gerar código de confirmação**.

Um código de confirmação será criado e exibido no bloco **Confirmar ações do usuário**.

8. Envie o código de confirmação para o usuário do Kaspersky Thin Client.

Para confirmar a alteração do certificado para conexão com o Kaspersky Security Center:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.

2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.

3. Na janela aberta, selecione a guia **Configurações do aplicativo**.

4. Selecione a seção **Troca de dados**.

5. No bloco **Confirmar ações do usuário**, insira o código a partir da interface do Kaspersky Thin Client que o usuário lhe enviou e clique em **Gerar código de substituição do certificado**.

Um código de substituição do certificado será criado e exibido no bloco **Confirmar ações do usuário**.

6. Envie o código de substituição do certificado para o usuário do Kaspersky Thin Client.

Gerenciamento dos certificados do Kaspersky Thin Client pelo Web Console

No Kaspersky Security Center, você pode acessar as funções de gerenciamento de [certificados](#) para conectar thin clients a um servidor de log e a um ambiente remoto. Na interface do Kaspersky Security Center Web Console, é possível exibir, [adicionar](#) e [excluir](#) esses certificados.

Recomendamos configurar a [conexão de thin clients no grupo de administração](#) para um servidor de log e para um ambiente remoto usando somente os certificados atribuídos pelo administrador no Web Console. Isso ajudará a impedir que o Kaspersky Thin Client se conecte a nós não confiáveis.

Esta seção também fornece [instruções sobre como gerenciar certificados para conectar o Kaspersky Thin Client ao Kaspersky Security Center](#).

Sobre um certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center

O Kaspersky Thin Client usa um *certificado de dispositivos móveis do usuário* (aqui também referido como "certificado") para se conectar com o Kaspersky Security Center. Para obter informações detalhadas sobre este e outros tipos de certificados usados pelo Kaspersky Security Center, consulte a [Ajuda on-line do Kaspersky Security Center](#) ².

Esse certificado é criado com o uso do *assistente de início rápido do Servidor de Administração* após a instalação do Kaspersky Security Center. O período de validade padrão de um certificado emitido é de um ano.

Os certificados de dispositivos móveis do usuário não são reemitidos automaticamente.

É possível [reemitir o certificado no Web Console](#) ou [criar um novo certificado](#) manualmente e [carregá-lo no Web Console](#).

Ao [migrar para um novo Servidor de Administração do Kaspersky Security Center](#), [crie um novo certificado manualmente](#) para carregá-lo no Servidor atual como um certificado reserva e, em seguida, no novo Servidor como o certificado principal.

Reemissão de um certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center com o uso do Web Console

O Kaspersky Thin Client usa um certificado de dispositivos móveis do usuário para conexão com o Kaspersky Security Center. Os certificados deste tipo não são reemitidos automaticamente.

Para reemitir um certificado para conectar o Kaspersky Thin Client ao Kaspersky Security Center na interface do Web Console:

1. No menu do Kaspersky Security Center Web Console, clique no botão  ao lado do Servidor de Administração do Kaspersky Security Center.
A janela de **Propriedades do Servidor de Administração** é aberta.
2. Selecione a subseção **Certificados**.
3. Na janela exibida, na seção **Autenticação do Servidor de Administração por dispositivos móveis**, selecione o certificado necessário e clique em **Reemitir**.
4. Na janela exibida, especifique o endereço do Servidor e indique quando ativar o certificado. Confirme sua escolha.
5. Clique em **Salvar** na janela exibida.

Certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center.

Os dispositivos incluídos em um [grupo de administração](#)  receberão o certificado reemitido para conexão com o Kaspersky Security Center após sincronização do Kaspersky Thin Client com o Kaspersky Security Center. O certificado reemitido será salvo no armazenamento de certificados do Kaspersky Thin Client e poderá ser usado como certificado reserva para conexão de thin clients com o Kaspersky Security Center quando o certificado atual expirar.

Também é possível [emitir manualmente um novo certificado](#) para conexão do Kaspersky Thin Client com o Kaspersky Security Center.

Criação de um certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center

É possível criar manualmente um [certificado](#) para conexão do Kaspersky Thin Client com o Kaspersky Security Center. O certificado criado pode ser usado como principal ou reserva, por exemplo, ao [migrar para um novo Servidor de Administração do Kaspersky Security Center](#).

Recomendamos ficar familiarizado com os requisitos de certificado do Kaspersky Security Center na [Ajuda on-line do Kaspersky Security Center](#).

O certificado criado deve ser [carregado no Web Console](#).

Para criar um certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center com o uso da ferramenta OpenSSL:

1. Inicie o console e vá para a pasta na qual deseja criar o certificado.

2. No console, inicie a ferramenta OpenSSL e execute o seguinte 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"
```

onde:

- `-keyout key.pem` é o nome do arquivo no qual a chave privada do certificado criado será salva.
- `-out server.pem` é o nome do arquivo no qual o certificado criado será salvo.
- `-days` é uma configuração que define o prazo de validade do certificado criado, em dias. Recomendamos configurar o prazo de validade do certificado para não mais que 397 dias.
- `-subj '/CN=mydomain.ru/C=RU/L=Moscow/O=My Organization Name/OU=My Organization Unit Name'` são dados da sua organização: nome do domínio, localização, nome.

3. Insira e confirme a senha da chave privada de certificado. Essa senha precisará ser inserida ao carregar o certificado do usuário para o Web Console como um certificado de dispositivos móveis. Comprimento mínimo da senha: 8 caracteres.

Então, os dois arquivos a seguir serão criados na pasta na qual o comando foi executado:

- O `server.pem` é um arquivo de certificado para conectar o Kaspersky Thin Client ao Kaspersky Security Center.
- O `key.pem` é uma chave privada do certificado para conectar o Kaspersky Thin Client ao Kaspersky Security Center.

Carregamento de um certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center usando o Web Console

Depois de [criar um certificado](#) para conexão do Kaspersky Thin Client com o Kaspersky Security Center, carregue esse certificado no Web Console para fazer a transferência para os thin clients adicionados ao [grupo de administração](#).

Recomendamos ficar familiarizado com os requisitos de certificado do Kaspersky Security Center na [Ajuda on-line do Kaspersky Security Center](#).

Para carregar um certificado ao Web Console para conectar o Kaspersky Thin Client ao Kaspersky Security Center:

1. No menu do Kaspersky Security Center Web Console, clique no botão  ao lado do Servidor de Administração do Kaspersky Security Center.
A janela de **Propriedades do Servidor de Administração** é aberta.
2. Selecione a subseção **Certificados**.
3. Na janela aberta, no bloco **Autenticação do Servidor de Administração por dispositivos móveis**, selecione **Outro certificado** e clique no botão **Gerenciar certificado**.
4. No painel aberto à direita, clique em **Procurar** e faça o seguinte:
5. Na lista suspensa **Tipo de certificado**, selecione o **Certificado X.509**:
 - a. Caso o certificado do usuário esteja protegido com uma senha, insira a senha.
 - b. Selecione o arquivo de certificado do usuário clicando no botão **Procurar** no bloco **Certificado**.
 - c. Selecione a chave privada para o certificado do usuário clicando no botão **Procurar** no bloco **Chave privada**.
6. Clique em **Salvar** para salvar o certificado que está sendo adicionado.
7. Clique em **Salvar** para salvar as alterações feitas na subseção **Certificados**.

O certificado para conexão do Kaspersky Thin Client com o Kaspersky Security Center será carregado no Web Console. Os dispositivos incluídos no grupo de administração recebem o novo certificado após a sincronização do Kaspersky Thin Client com o Kaspersky Security Center.

Adição de novos certificados no Web Console

No Web Console, é possível adicionar [certificados](#) para se conectar a um ambiente remoto ou a um servidor de log. Para fazer isso, o thin client deve ser [adicionado a um grupo de administração](#).

Depois de adicionar um certificado para um thin client no Web Console, todos os certificados que foram aceitos anteriormente por um usuário serão removidos do armazenamento de certificados do dispositivo.

Para adicionar novos certificados pelo Web Console:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Certificados**.
5. Na tabela **Certificados válidos**, clique no botão **Adicionar** na parte superior da tabela.
6. No painel aberto à direita, selecione todos os certificados que foram carregados anteriormente e selecione os novos certificados. O tamanho total dos arquivos carregados não deve exceder 1 MB. É possível carregar os certificados somente no formato DER. Cada arquivo de certificado deve conter apenas um certificado. Caso necessário, é possível [converter os certificados do formato PEM para DER](#) com antecedência.
7. Clique em **OK** para confirmar o carregamento dos certificados selecionados.

Os certificados selecionados serão carregados e as informações sobre eles serão exibidas na tabela **Certificados válidos**.

Caso o certificado adicionado seja um certificado raiz, a conexão somente será estabelecida de acordo com o nome de domínio do servidor.

Remoção dos certificados do Web Console

No Web Console, é possível remover os certificados atribuídos aos thin clients em um [grupo de administração](#) @.

Se você remover todos os certificados que foram [atribuídos a um grupo de thin clients](#), os dispositivos desse grupo poderão se conectar a qualquer servidor, incluindo servidores aos quais nenhum certificado foi atribuído.

Para remover certificados:

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no [nome da política](#) do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configurações do aplicativo**.
4. Selecione a seção **Certificados**.
5. Na tabela **Certificados válidos**, marque as caixas de seleção ao lado dos certificados que precisa remover.
6. Clique em **Excluir** e confirme a exclusão.

Os certificados selecionados serão removidos.

Conversão de um certificado do formato PEM para DER

O Kaspersky Security Management Suite oferece suporte ao carregamento de certificados somente no formato DER. É possível converter um arquivo de certificado do formato PEM para DER.

Para executar essas instruções no computador local, é preciso ter a ferramenta OpenSSL.

Para converter um arquivo de certificado do formato PEM para DER:

1. Inicie o console no computador local.
2. Vá para a pasta que contém o arquivo de certificado PEM e execute o seguinte comando de conversão de arquivo:

```
openssl x509 -outform der -in <nome do arquivo de certificado>.pem -out <nome do arquivo de certificado>.der
```

onde:

 - <nome do arquivo de certificado>.pem é o nome do arquivo de certificado original no formato PEM.
 - <nome do arquivo de certificado>.der é o nome do arquivo de certificado convertido no formato DER.

O novo arquivo de certificado no formato DER será gerado nesta mesma pasta.

Atualização de um certificado ao migrar para um novo servidor do Kaspersky Security Center

Para [migrar thin clients para um novo Servidor de Administração do Kaspersky Security Center](#), emita um [certificado](#) para salvá-lo no servidor do Kaspersky Security Center como reserva e, em seguida, use-o no novo servidor como o certificado principal.

Para emitir e preparar um novo certificado:

1. Inicie o console e vá para a pasta na qual deseja criar o certificado.
2. Inicie o utilitário OpenSSL e emita o certificado usando o seguinte comando:

```
openssl req -x509 -sha256 -nodes -days 397 -newkey rsa:2048 -keyout <nome do arquivo de chave>.key -out <nome do arquivo de certificado>.crt
```

O certificado gerado e os arquivos de chave são salvos localmente.
3. Empacote o certificado e a chave em um contêiner usando o seguinte comando:

```
openssl pkcs12 -export -out <nome do contêiner>.pfx -inkey <nome do arquivo de chave>.key -in <nome do arquivo de certificado>.crt
```
4. Insira e repita a senha para o contêiner. Essa senha é necessária ao carregar o certificado nos servidores.

Como resultado, o arquivo contêiner no formato PFX é salvo localmente.

Para carregar um certificado no servidor do Kaspersky Security Center atual como reserva:

1. Vá para o diretório no qual o Kaspersky Security Center está instalado e inicie o console.
2. Execute o utilitário klsetsrvcert e insira o seguinte comando:

```
klsetsrvcert -t MR -i <caminho para o contêiner> -p <senha do contêiner> -o NoCA
```

Não é preciso baixar o utilitário klsetsrvcert. O utilitário está incluído no kit de distribuição do Kaspersky Security Center.

Após a execução do comando, o Kaspersky Security Center é reiniciado.

O [certificado de reserva](#) é carregado no Web Console.

Para carregar o certificado para um novo servidor do Kaspersky Security Center como o principal:

No console, inicie o utilitário klsetsrvcert e execute o seguinte comando:

```
klsetsrvcert -t M -i <caminho para o contêiner> -p <senha do contêiner> -o NoCA
```

Após a execução das instruções acima, o certificado para conexão com o novo Servidor de Administração do Kaspersky Security Center será atualizado.

Monitoramento de eventos do Kaspersky Thin Client pelo Kaspersky Security Center Web Console

Esta seção contém instruções sobre o monitoramento de eventos registrados no Kaspersky Thin Client pelo Kaspersky Security Center Web Console.

Configuração do registro das notificações de eventos do Kaspersky Thin Client por meio do Kaspersky Security Center Web Console

O Kaspersky Security Center permite receber informações sobre eventos que ocorrem enquanto o Kaspersky Thin Client estiver em execução. Na interface do Kaspersky Security Center Web Console, é possível configurar uma notificação sobre o registro desses eventos. Cada evento no Kaspersky Security Center tem um nível próprio de importância. Dependendo das condições da sua ocorrência, um evento pode receber um dos seguintes níveis de importância:

- Um evento *crítico* é um evento que indica a ocorrência de um problema crítico que pode levar à perda de dados, ao mau funcionamento operacional ou a um erro crítico.
- Uma *falha funcional* é um evento que indica a ocorrência de um problema, erro ou mau funcionamento sério que ocorreu durante a operação do aplicativo ou durante a execução de um procedimento.

- Uma *advertência* é um evento que requer atenção porque enfatiza situações importantes na operação do Kaspersky Thin Client e pode indicar um possível problema no futuro. A maioria dos eventos é designada como advertências se o aplicativo puder ser restaurado sem perda de dados ou recursos funcionais após a ocorrência desses eventos.
- Uma *informações* é um evento que fornece informações quanto à conclusão bem-sucedida de uma operação, o funcionamento adequado do aplicativo ou a conclusão de um procedimento.

É possível configurar as notificações sobre os eventos do Kaspersky Thin Client no Kaspersky Security Center Web Console para um dispositivo ou um grupo de dispositivos.

Como configurar as notificações de eventos para um dispositivo

1. Na janela principal do Kaspersky Security Center Web Console, execute uma das seguintes ações:

- Se o thin client estiver incluído em um grupo de administração, selecione **Ativos (dispositivos)** → **Dispositivos gerenciados**.
- Se o thin client não tiver sido adicionado a um grupo de administração, selecione **Descoberta e implementação** → **Dispositivos não atribuídos**.

2. Clique no nome do dispositivo no qual o Kaspersky Thin Client está em execução. É possível visualizar o nome do dispositivo na [interface do Kaspersky Thin Client](#).

3. Na janela aberta, selecione a guia **Aplicativos**.

4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.

Uma janela contendo as informações sobre o Kaspersky Thin Client será aberta.

5. Selecione a guia **Configuração de eventos**.

6. Selecione a importância dos eventos cujas informações você deseja receber:

- **Crítico**
- **Falha funcional**
- **Advertência**
- **Informações**

Será exibida uma tabela de eventos para o nível de importância selecionado.

7. Clique no botão **Adicionar evento** e, na janela aberta, marque a caixa de seleção ao lado dos tipos de eventos que deseja adicionar.

8. Clique em **OK**.

9. Para salvar as alterações, clique no botão **Salvar**.

O Kaspersky Thin Client enviará os tipos de eventos selecionados com a importância especificada para o Servidor de Administração do Kaspersky Security Center. O tempo de armazenamento padrão dos eventos é de 30 dias.

Como configurar notificações de eventos para dispositivos em um grupo de administração

1. Na janela principal do Web Console, selecione **Ativos (Dispositivos)** → **Políticas e perfis**.
2. Clique no nome da política do plug-in da Web do Kaspersky Security Management Suite.
3. Na janela aberta, selecione a guia **Configuração de eventos**.
4. Selecione a importância dos eventos cujas informações você deseja receber:

- **Crítico**
- **Falha funcional**
- **Advertência**
- **Informações**

Será exibida uma tabela de eventos para o nível de importância selecionado.

5. Clique no botão **Adicionar evento** e, na janela aberta, marque a caixa de seleção ao lado dos tipos de eventos que deseja adicionar.
6. Clique em **OK**.
7. Para salvar as alterações, clique no botão **Salvar**.

Caso o botão de alternância **Aplicado** seja desativado, as configurações não serão aplicadas aos dispositivos Kaspersky Thin Client que estão no grupo de administração e são atendidos pela política de segurança atual.

O Kaspersky Thin Client enviará os tipos de eventos selecionados com a importância especificada para o Servidor de Administração do Kaspersky Security Center. O tempo de armazenamento padrão dos eventos é de 30 dias.

Para obter as informações detalhadas sobre a configuração das notificações para registro de eventos no Kaspersky Security Center Web Console, consulte a [Ajuda on-line do Kaspersky Security Center](#).

Exibição dos eventos do Kaspersky Thin Client no Web Console

É possível visualizar os eventos registrados pelo Kaspersky Thin Client no Web Console.

Para visualizar os eventos registrados pelo Kaspersky Thin Client no Web Console:

1. Na janela principal do Kaspersky Security Center Web Console, execute uma das seguintes ações:

- Se o thin client estiver incluído em um grupo de administração, selecione **Ativos (dispositivos)** → **Dispositivos gerenciados**.
- Se o thin client não tiver sido adicionado a um grupo de administração, selecione **Descoberta e implementação** → **Dispositivos não atribuídos**.

2. Clique no nome do dispositivo relevante. O nome do dispositivo é indicado na [interface do Kaspersky Thin Client](#).

3. Na janela aberta, selecione a guia **Eventos**.

Uma janela exibindo uma tabela de eventos registrados é aberta. As seguintes informações são exibidas para cada evento:

- **Hora** mostra a data e a hora nas quais o Web Console recebeu o evento registrado pelo Kaspersky Thin Client.
- **Evento** exibe um tipo do evento.
- **Descrição** exibe uma descrição curta do evento registrado.
- **Aplicativo** exibe um nome do aplicativo para o qual o evento foi recebido no Web Console.
- **Número da versão** exibe uma versão do aplicativo para a qual o evento foi recebido no Web Console.
- **O nível de importância** exibe a gravidade do evento.
- **Tarefa** exibe um nome da tarefa a ser executada quando o evento é registrado.
- **Registrado** exibe a data e a hora em que o evento foi registrado pelo Kaspersky Thin Client.

Solução de problemas

Se ocorrer um erro, verifique se:

1. [O thin client está ativado.](#)
2. [O thin client está conectado na rede.](#)
3. [O endereço IP ou nome do servidor, nome de usuário e senha corretos foram inseridos ao se conectar no ambiente remoto.](#)

Caso não consiga resolver o erro, entre em contato com o [Suporte Técnico](#). Caso necessário, os especialistas do Suporte Técnico poderão solicitar o fornecimento de informações sobre o sistema ou [logs de eventos e auditoria](#).

Reconectar após uma falha de conexão remota

Em caso de falha na conexão entre o Kaspersky Thin Client e o ambiente remoto, uma reconexão automática será iniciada, desde que esse recurso esteja ativado na configuração de conexão remota.

Se a conexão não for restaurada durante a tentativa de reconexão ou se a conexão automática for recusada, a tela da sessão remota será fechada e uma mensagem indicando a causa do mau funcionamento aparecerá.

Para retomar a sessão remota:

1. Feche a mensagem de erro.
2. Tente se conectar ao ambiente remoto.
3. Caso não consiga estabelecer a conexão, entre em contato com seu administrador para obter ajuda na resolução de possíveis problemas na rede física que possam estar impedindo o Kaspersky Thin Client de se conectar ao desktop remoto.
4. Se a conexão direta tiver sido estabelecida, mas ainda assim não conseguir conectar-se com o desktop remoto, entre em contato com o [Suporte Técnico](#).

Problemas de restrição de acesso às funções do plug-in da web do Kaspersky Security Management Suite

Depois de [instalar](#) ou [atualizar](#) o plug-in da web do Kaspersky Security Management Suite, os [usuários com o conjunto completo de direitos](#) talvez não tenham acesso a algumas funções do aplicativo.

Para corrigir problemas com o acesso compartilhado às funções do plug-in da web:

1. Coloque o arquivo RBAC do [kit de distribuição do plug-in da web](#) nos seguintes diretórios no [Servidor de Administração](#):

a. <diretório de instalação do Kaspersky Security Center>/rbac

b. /var/opt/kaspersky/klnagent_srv/1093/dat/rbac

2. Reinicie o Servidor de Administração.

Os usuários devem receber os direitos de acessar as funções do plug-in da web de acordo com suas funções.

Caso não consiga resolver o problema, entre em contato com o [Suporte Técnico](#).

Entrando em contato com o Suporte Técnico

Caso tenha problemas que [não possa resolver sozinho](#) durante a operação com o Kaspersky Thin Client, entre em contato com o [Suporte Técnico da Kaspersky](#).

Antes de entrar em contato com o Suporte Técnico, certifique-se de ler o [Regulamento de Suporte Técnico](#).

Ao entrar em contato com o Suporte Técnico, os especialistas podem solicitar o fornecimento de [logs de auditoria e de eventos](#). Na interface do Kaspersky Thin Client, você pode [encaminhar logs para um servidor de log](#) implementado na infraestrutura de sua organização, de onde os especialistas da Kaspersky possam baixá-los.

Informações sobre os logs do Kaspersky Thin Client

O Kaspersky Thin Client mantém dois tipos de logs:

- Log de eventos. Esse registro salva todos os [eventos](#) registrados pelos componentes do Kaspersky Thin Client. É possível visualizar o log de eventos na interface do Kaspersky Thin Client e [encaminhá-lo para um servidor de log](#).
- Log de auditoria. Esse registro armazena eventos importantes na operação do thin client, como a interação com certificados para se conectar ao Kaspersky Security Center, informações sobre o Servidor de Administração e conexões ou desconexões dele, além de redefinições de fábrica do dispositivo. O log de auditoria não pode ser exibido na interface do Kaspersky Thin Client. É possível [encaminhar o arquivo de log de auditoria para um servidor de log](#).

Log de eventos

O log de eventos do Kaspersky Thin Client contém as seguintes informações:

- Data e hora em que o evento ocorreu.
- Nome do componente do Kaspersky Thin Client que registrou o evento.
- Gravidade do evento. Os seguintes valores são possíveis:
 - *Trace* são todas as mensagens e advertências possíveis que ocorrem durante a operação do aplicativo.
 - *Debug* são mensagens de depuração, todas as mensagens informativas e importantes e todos as advertências e mensagens sobre erros comuns e críticos.
 - *Info* são mensagens informativas, mensagens importantes e todos as advertências e mensagens sobre erros comuns e críticos.
 - *Warn* são todos os avisos e mensagens sobre erros comuns e críticos.
 - *Error* são mensagens sobre erros e erros críticos na operação do aplicativo.
 - *Fatal* são mensagens sobre erros críticos na operação do aplicativo.

- Informações de depuração em <Arquivo>:<Número da linha>, formato de <Função>, onde:
 - *File* é um nome de arquivo.
 - *Line Number* é o número da linha no arquivo.
 - *Function* são as informações de depuração.
- ID do processo e ID do encadeamento.
- ID da versão do produto.

Log de auditoria

O log de auditoria do Kaspersky Thin Client contém os seguintes eventos e detalhes de eventos:

- Adição, substituição e alternância de certificados para conexão com o Kaspersky Security Center na interface do Kaspersky Thin Client:
 - data e hora do evento;
 - endereço IP e/ou nome de domínio do Servidor de Administração do Kaspersky Security Center;
 - número da porta do Servidor de Administração do Kaspersky Security Center;
 - ID do thin client;
 - lista de atributos do certificado: nome do emissor, nome do assunto, impressão digital do certificado, data e hora de início de validade, data e hora de término de validade.
- Ativação (manual e automaticamente) e desativação do gerenciamento do Kaspersky Thin Client por meio do Kaspersky Security Center:
 - data e hora do evento;
 - endereço IP e/ou nome de domínio do Servidor de Administração do Kaspersky Security Center;
 - número da porta do Servidor de Administração do Kaspersky Security Center;
 - ID do thin client.
- Redefinição de fábrica do Kaspersky Thin Client:
 - data e hora do evento;
 - ID do thin client.
- Aceitação de uma conexão remota ao thin client:
 - data e hora do evento;
 - endereço IP e/ou nome de domínio do usuário que se conectou ao thin client;
 - nome do usuário que se conectou ao thin client.

- Criação de um novo arquivo de log de auditoria em caso de rotação de log:
 - data e hora do evento;
 - ID do thin client;
 - versão do Kaspersky Thin Client.
- Salvamento e exclusão da senha do usuário para a conexão automática a um ambiente remoto:
 - data e hora do evento;
 - nome de usuário para se conectar ao ambiente remoto.

Encaminhamento do log

Ao entrar em [contato com o Suporte Técnico](#), os especialistas da Kaspersky podem solicitar que você forneça [logs de eventos e de auditoria](#). Na interface do Kaspersky Thin Client, você pode encaminhar logs para um servidor de log, de onde os especialistas possam baixá-los.

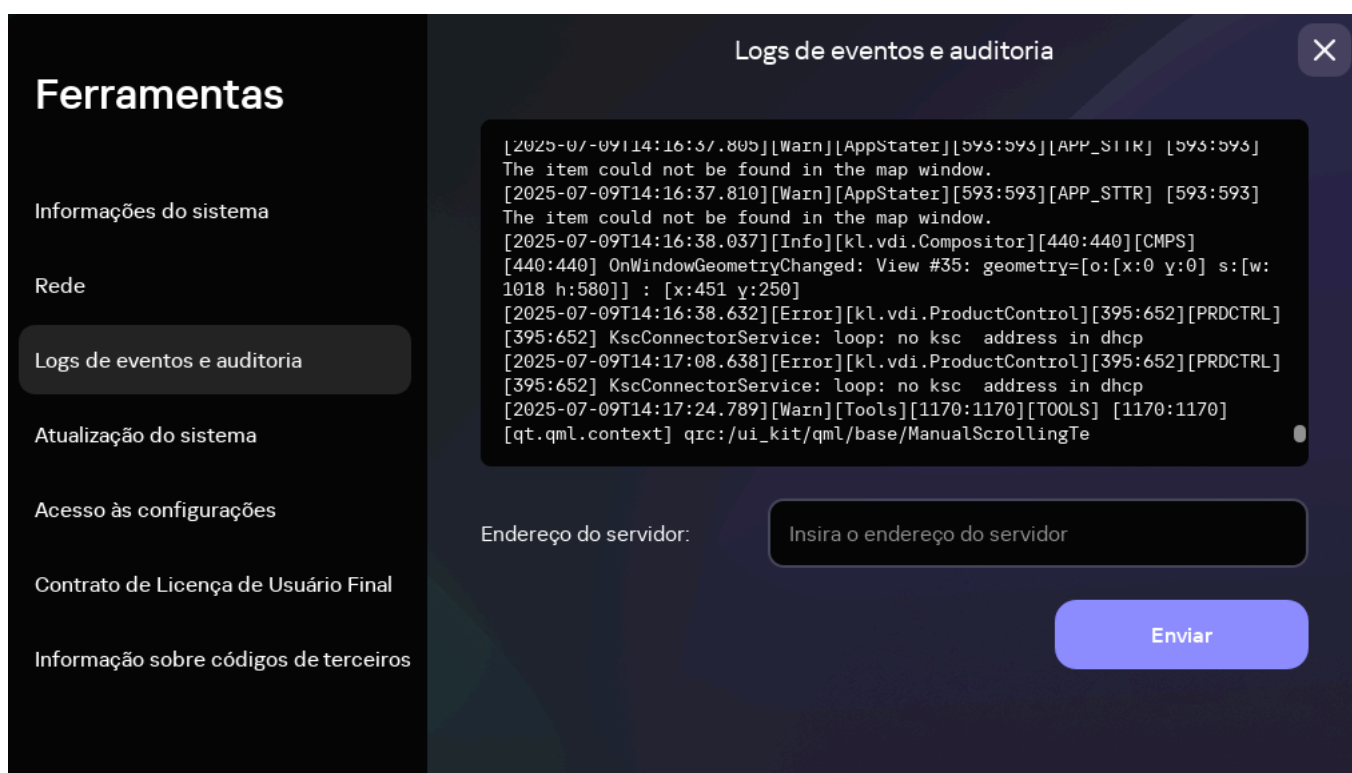
O [servidor de log](#) deve primeiro ser implementado na infraestrutura de sua organização. Para obter informações detalhadas sobre a implementação do servidor, consulte o guia do administrador desse servidor.

Os tamanhos máximos de arquivo para o log de eventos e o log de auditoria são 150 MB e 512 MB, respectivamente. Quando o tamanho do arquivo de log de evento ou de auditoria atinge seu limite correspondente, o Kaspersky Thin Client exclui os logs existentes e começa a gravar os novos. Sempre que os logs de evento e de auditoria forem atualizados, a versão atual do Kaspersky Thin Client é registrada no início do log.

Para encaminhar os logs de auditoria e de eventos do Kaspersky Thin Client:

1. No painel de controle do Kaspersky Thin Client, clique em  e selecione **Ferramentas** no menu aberto.
2. Na janela aberta, selecione a seção **Logs de eventos e auditoria** (consulte a figura abaixo).

Esta seção exibe as entradas do log de eventos. As entradas do log de auditoria não são exibidas na interface do Kaspersky Thin Client.



Ferramentas. Seção Logs de eventos e auditoria

As informações sobre os eventos registrados do Kaspersky Thin Client são exibidas.

3. No campo **Endereço do servidor**, insira o endereço do servidor de destino que deve receber os logs de auditoria e de eventos e clique no botão **Enviar**.

Caso o thin client pertença a um [grupo de administração](#), o endereço do servidor de log poderá ser [aplicado pelo Web Console](#). Se esse for o caso, não será possível mudar isso na interface do Kaspersky Thin Client.

Recomendamos verificar o endereço correto do servidor de destino para o qual os logs estão sendo enviados. Caso o endereço errado seja indicado, os logs poderão ficar expostos para terceiros.

4. Na janela aberta, confirme se deseja encaminhar os logs de auditoria e de eventos.

Caso o dispositivo não seja membro de um [grupo de administração](#) e esta for a primeira vez que você estiver enviando logs de eventos e auditoria para o servidor de logs, será exibida uma janela solicitando a adição de um [certificado para conexão com o servidor de log](#).

Verifique as configurações do certificado que está sendo adicionado e clique no botão **Adicionar certificado**. O certificado será adicionado ao armazenamento de certificados do sistema do Kaspersky Thin Client e será usado para conexões subsequentes.

Os logs de auditoria e de eventos do Kaspersky Thin Client serão encaminhados para o servidor especificado.

Glossário

Administrador do Kaspersky Security Center

Pessoa que gerencia as operações do thin client pelo sistema de administração centralizado remoto conhecido como Kaspersky Security Center.

Ambiente remoto

Qualquer recurso remoto compatível, como um desktop remoto ou aplicativo virtual, que um usuário thin client pode acessar para trabalhar usando tecnologia de acesso remoto.

Aplicativo virtual

Aplicativo implementado em um servidor remoto e que requer o uso de tecnologias de acesso remoto para se conectar com ele.

Broker

Serviço que controla o acesso e as conexões com as áreas de trabalho remotas e aplicativos (por exemplo, Microsoft Remote Desktop Connection Broker).

Desktop remoto

Um sistema operacional instalado em um computador ou implementado em um ambiente virtual. As tecnologias de acesso remoto são usadas para se conectar com esse tipo de sistema operacional.

Evento

Uma entrada contendo os registros de alterações feitas no estado ou configuração de um thin client ou erros que requerem a atenção de um administrador do sistema.

Grupo de administração

Um conjunto de dispositivos gerenciados pelo Kaspersky Security Center e agrupados por função. Os dispositivos são agrupados para facilitar o gerenciamento como um todo. Um grupo pode incluir outros grupos. Para cada dispositivo adicionado ao grupo, é possível criar políticas e tarefas de grupo que serão aplicadas a todos os dispositivos.

Plug-in da Web do Kaspersky Security Management Suite

Componente especializado que fornece uma interface para gerenciar as configurações do Kaspersky Thin Client pelo Kaspersky Security Center Administration Console.

Política

Uma política determina as configurações do Kaspersky Thin Client e define o acesso à definição de configurações do sistema Kaspersky Thin Client em dispositivos em um grupo de administração. É possível criar um número ilimitado de políticas diferentes para o Kaspersky Thin Client instalado em dispositivos de cada grupo de administração, mas apenas uma política por vez poderá ser aplicada a cada dispositivo Kaspersky Thin Client em um grupo de administração.

Servidor de Administração

Componente do aplicativo Kaspersky Security Center que fornece armazenamento e gerenciamento centralizados das informações sobre os aplicativos da Kaspersky instalados na rede de uma empresa.

Servidor de log

O servidor que receberá os [logs de eventos e de auditoria](#) do Kaspersky Thin Client. Esse servidor está implementado em sua rede corporativa.

Sessão remota

Sessão de trabalho no ambiente remoto ao qual o usuário se conectou por meio da interface do thin client.

Thin client

Um computador pessoal compacto usado para conexão por uma rede aos servidores remotos que fornecem armazenamento de dados e têm todos os aplicativos necessários instalados para uma operação. Periféricos, como monitor, teclado e mouse, são conectados ao thin client.

TLS

Protocolo seguro que usa criptografia para transferir os dados em redes locais e na Internet.

Informação sobre códigos de terceiros

As informações sobre códigos de terceiros estão contidas no arquivo denominado `LegalNotices_en.txt` que está incluído no kit de distribuição.

Também é possível visualizar as informações sobre códigos de terceiros na interface do Kaspersky Thin Client.

Para visualizar a informação sobre códigos de terceiros,

no painel de controle do Kaspersky Thin Client, clique em  e selecione **Ferramentas → Informação sobre códigos de terceiros** no menu aberto.

Uma janela que mostra as informações sobre o uso de código de terceiros será aberta na versão atual do Kaspersky Thin Client.

Avisos de marcas comerciais

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

Ubuntu é uma marca registrada da Canonical Ltd.

Citrix, Citrix Workspace são marcas registradas ou marcas comerciais do Cloud Software Group, Inc. e/ou suas subsidiárias nos Estados Unidos e/ou em outros países.

Dell e outras marcas comerciais são marcas comerciais da Dell Inc. ou de suas subsidiárias.

Linux é a marca comercial da Linus Torvalds nos Estados Unidos e em outros países.

Microsoft, RemoteFX, Windows e Windows Server são marcas comerciais registradas do grupo de empresas Microsoft.

OpenSSL é uma marca comercial de propriedade da OpenSSL Software Foundation.

JavaScript é a marca comercial da Oracle e/ou de suas afiliadas.