kaspersky

Kaspersky Thin Client

Índice

Ajuda do Kaspersky Thin Client

	Novidades Descubra as novidades desta versão do Kaspersky Thin Client.		**Requisitos de hardware e software** Verifique os requisitos para os ambientes remotos e os dispositivos periféricos conectados.
	Atualização Como atualizar a versão do Kaspersky Thin Client.		**Redefinição de configurações e dados** Como redefinir as configurações e os dados do Kaspersky Thin Client.
	Primeiros passos Iniciando o thin client. Configuração inicial e conexão com o Kaspersky Security Center. Atribuir certificados.		**Configuração e conexão com um ambiente remoto** Opções de conexão disponíveis. Conexão com um ambiente remoto. Definir as configurações do Kaspersky Thin Client e as configurações de conexão para ambientes remotos e o Kaspersky Security Center. Configurar thin clients usando o Kaspersky Security Center.
	Recursos avançados Gerenciamento de certificados do Kaspersky Thin Client. Gerenciamento de políticas. Gerenciamento do acesso às configurações do Kaspersky Thin Client.		**Monitoramento de eventos** Visualizar e encaminhar logs de eventos e de auditoria para um servidor de log. Visualizar eventos do Kaspersky Thin Client usando o Kaspersky Security Center Web Console.

Sobre o Kaspersky Thin Client

O Kaspersky Thin Client versão 2.0 (também denominado "Kaspersky Thin Client" ou "o sistema") é um sistema operacional para thin clients baseados no sistema operacional KasperskyOS. O Kaspersky Thin Client foi criado para fornecer aos usuários acesso ao desktop remoto e serve como um substituto para uma estação de trabalho local. O Kaspersky Thin Client versão 2.0 pode ser instalado somente em thin clients TONK TN1200 ou Centerm F620.

Funções principais do Kaspersky Thin Client:

- Conectar com desktops remotos e virtuais que executam sistemas operacionais Microsoft® Windows® com o uso do Protocolo da Área de Trabalho Remota (RDP) e o Microsoft Remote Desktop Connection Broker com acesso por meio de nome de usuário e senha.
- Conectar com servidores de terminal que executam os sistemas operacionais Microsoft Windows Server® com o uso do Protocolo da Área de Trabalho Remota (RDP) e o Microsoft Remote Desktop Connection Broker com acesso por meio de nome de usuário e senha.
- Conectar com desktops remotos e virtuais que executam sistemas operacionais Linux® com o uso do Protocolo da Área de Trabalho Remota (RDP) acesso por meio de nome de usuário e senha.
- Conectar os aplicativos virtuais pelo protocolo RDP via Microsoft Remote Desktop Connection Broker com acesso por meio de nome de usuário e senha.
- Conectar com desktops virtuais implementados na infraestrutura de desktop virtual do Basis.WorkPlace com autorização por nome de usuário e senha.
- Conectar com desktops virtuais implementados em uma infraestrutura Citrix Workspace ou VMware Horizon no aplicativo Web Access.
- Transmitir a imagem da tela do desktop remoto para o monitor conectado ao Kaspersky Thin Client.
- Redirecione um teclado e um mouse conectados ao Kaspersky Thin Client para um ambiente remoto.
- Redirecione unidades USB, cartões inteligentes, tokens USB, impressoras, microfone e dispositivos de reprodução de áudio conectados ao Kaspersky Thin Client para o ambiente remoto.
- Controlar, atualizar e monitorar de forma centralizada o Kaspersky Thin Client pelo Kaspersky Security Center Web Console versão 14.2. O plug-in da Web do Kaspersky Security Management Suite incluído no kit de distribuição é usado para a comunicação entre o Kaspersky Thin Client e o Kaspersky Security Center.

Kit de distribuição

O Kaspersky Thin Client 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:

- Arquivo comprimido que contém a imagem de instalação do Kaspersky Thin Client: Kaspersky_Thin_Client_<número da versão>.tar.gz.

- Pacote de inicialização: KTC_uboot_<número da versão>.tar.gz.
- Script para instalação no thin client: hw_install.sh.
- O arquivo de texto que contém as informações sobre códigos de terceiros: KTC_LegalNotices_en.txt.
- Os arquivos de texto que descrevem novos recursos e limitações conhecidas:
  - ReleaseNotes_Kaspersky_Thin_Client_<número da versão>_EN.txt.
  - ReleaseNotes_Kaspersky_Thin_Client_<número da versão>_ES.txt.
  - ReleaseNotes_Kaspersky_Thin_Client_<número da versão>_PT_BR.txt.
  - ReleaseNotes_Kaspersky_Thin_Client_<número da versão>_RU.txt.
- Os arquivos do Contrato de Licença de Usuário Final do Kaspersky Thin Client:
  - eula_en_ktc_<número da versão>.txt.
  - eula_es_ktc_<número da versão>.txt.
  - eula_pt_ktc_<número da versão>.txt.
  - eula_ru_ktc_<número da versão>.txt.

O kit de distribuição do Kaspersky Security Management Suite versão 2.0 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.

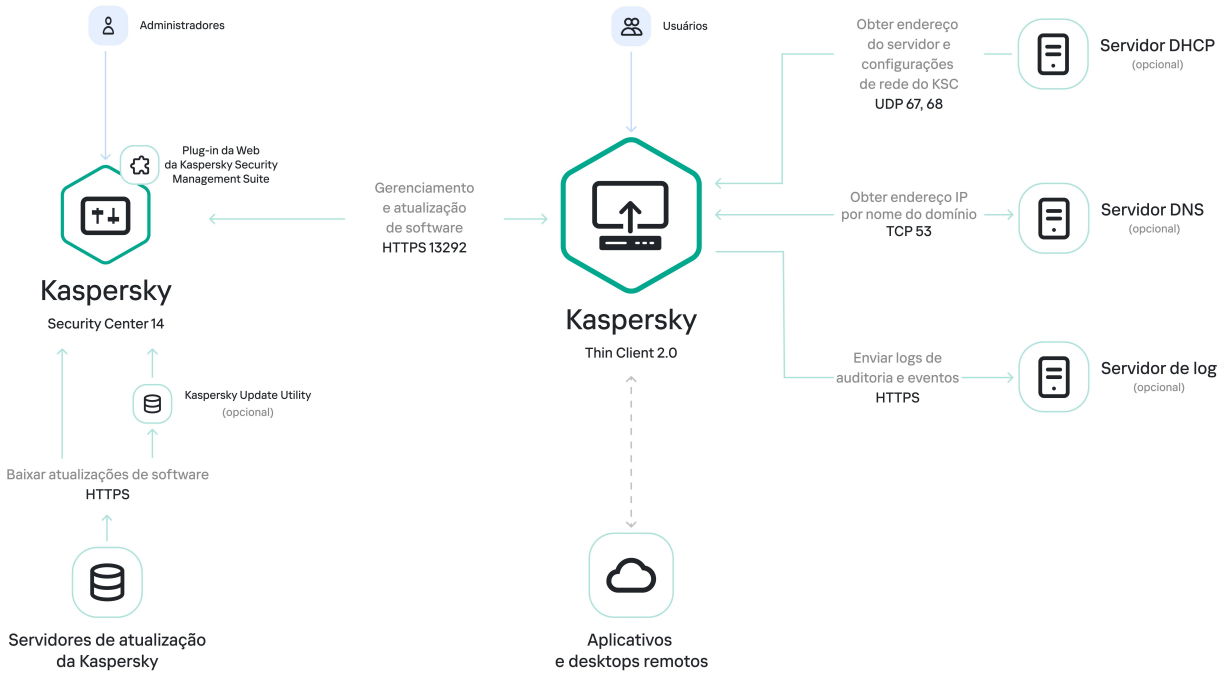
- Os arquivos do Microsoft Windows que contêm as imagens de instalação e os arquivos de assinatura do plug-in da Web para o Kaspersky Security Center Web Console:
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número da versão do plug-in>_en.exe.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número da versão do plug-in>_es.exe.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número da versão do plug-in>_pt_br.exe.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número da versão do plug-in>_ru.exe.
- Os 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 Console:
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número da versão do plug-in>_en.sh.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número da versão do plug-in>_es.sh.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número da versão do plug-in>_pt_br.sh.
  - Web_Plugin_Kaspersky_Security_Management_Suite_<número da versão do plug-in>_ru.sh.

- O arquivo de texto que contém as informações sobre códigos de terceiros para o Kaspersky Security Management Suite: KSMS_LegalNotices_en.txt.
- Os arquivos do Contrato de Licença de Usuário Final do Kaspersky Security Management Suite:
  - eula_en_ksms_<número da versão>.txt.
  - eula_es_ksms_<número da versão>.txt.
  - eula_pt_ksms_<número da versão>.txt.
  - eula_ru_ksms_<número da versão>.txt.

Operação do Kaspersky Thin Client

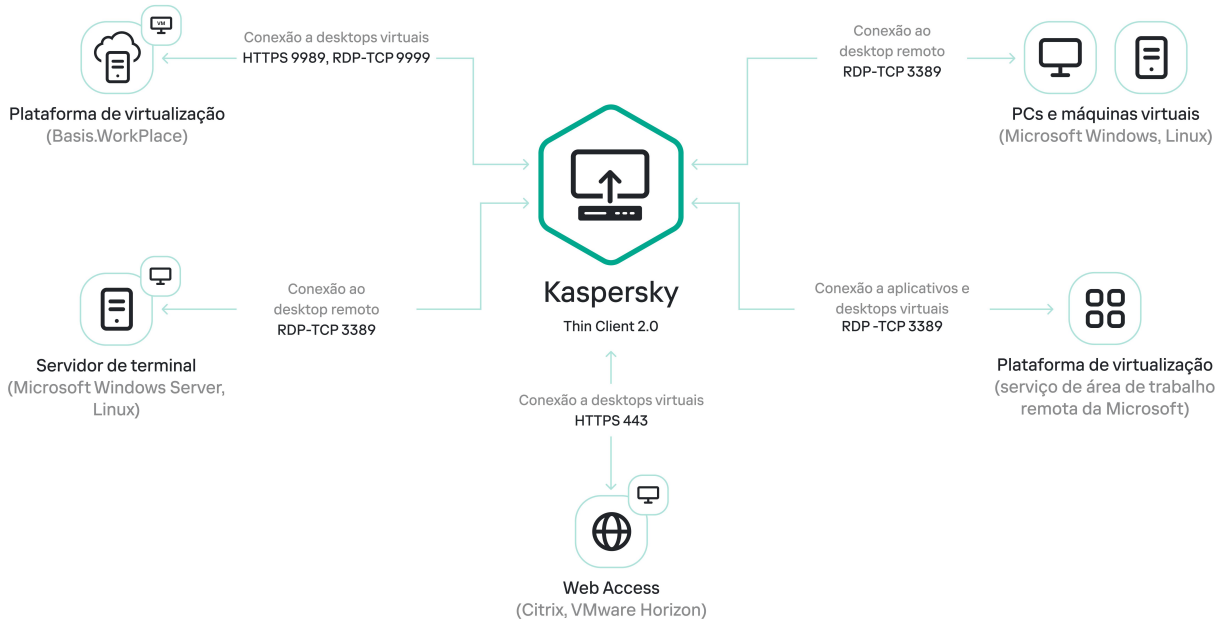
O cenário operacional padrão do Kaspersky Thin Client (consulte a figura abaixo) envolve os seguintes aspectos:

- Depois que o Kaspersky Thin Client é instalado na plataforma de hardware apropriada, ele recebe as configurações de rede de um servidor DHCP ou o administrador define manualmente essas configurações.
- O administrador conecta e configura a interação entre o Kaspersky Thin Client e o Kaspersky Security Center.
- O Kaspersky Thin Client recebe as configurações de conexão do desktop remoto ou do aplicativo virtual (doravante referido como sessão de conexão), as atualizações, os certificados confiáveis, além da data e hora juntamente com a política do Kaspersky Security Center.
- O usuário estabelece conexão com um desktop remoto ou aplicativo virtual por RDP.
- O usuário se conecta ao desktop remoto pela plataforma de virtualização Basis.WorkPlace.
- O usuário se conecta ao ambiente remoto no Web Access.
- Na interface do Kaspersky Thin Client, o usuário envia os logs de auditoria e de eventos para um servidor de log destinatário.
- O Kaspersky Thin Client usa o Kaspersky Security Center para receber atualizações de software do Servidor de atualização Kaspersky.



Cenário operacional padrão do Kaspersky Thin Client

A imagem abaixo exibe um diagrama de comunicação entre o Kaspersky Thin Client e as plataformas de virtualização.



Comunicação entre o Kaspersky Thin Client e as plataformas de virtualização

Requisitos de hardware e software

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

Requisitos para monitores conectados ao Kaspersky Thin Client

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

O Kaspersky Thin Client é compatível com as seguintes resoluções de monitor:

- 1024x768
- 1280x800
- 1280x1024
- 1366x768
- 1440x900
- 1600x900
- 1680x1050
- 1920x1080
- 1920x1200. Ao conectar um monitor com essa resolução, a resolução real exibida não será superior a 1920x1080.

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:

- Teclado e mouses com fio padrão sem funcionalidade multimídia conectados via portas USB.
- Unidades USB, cartões inteligentes e tokens conectados por portas USB.
- Impressoras conectadas pelas portas USB. O ambiente remoto deve ter o driver instalado da impressora conectada ao thin client.
- Dispositivos de registro e reprodução de áudio com fio conectados via miniconector.

Requisitos para desktops remotos

É possível se conectar aos computadores remotos, máquinas virtuais e servidores de terminal por meio de um dos seguintes sistemas operacionais instalados:

- Microsoft Windows 7
- Microsoft Windows 10

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

Requisitos para desktops remotos Basis.WorkPlace

O Kaspersky Thin Client é compatível com a operação da plataforma de virtualização Basis.WorkPlace versão 1.96. É possível usar o broker Basis.WorkPlace para se conectar com desktops remotos que executam um dos seguintes sistemas operacionais:

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

Requisitos de 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 o Kaspersky Security Center versões 14.2. 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 para servidores de logs de eventos

O servidor de log que receberá os logs de auditoria e de eventos do Kaspersky Thin Client é implementado na infraestrutura da empresa pelos especialistas do cliente.

O servidor de log tem os 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 um servidor de log destinatário por meio do método PUT.

Métodos de conexão remota

Esta seção contém informações sobre as tecnologias e os ambientes de acesso remoto compatíveis com Kaspersky Thin Client, bem como os métodos de conexão com esses ambientes. Esta seção fornece informações sobre quais dispositivos conectados com o Kaspersky Thin Client podem ser redirecionados para um ambiente remoto.

Conexão por 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.

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.

Antes de se conectar a um desktop remoto baseado em Linux usando um servidor xRDP que não tenha a extensão Kaspersky USB Redirector instalada, primeiro descubra qual versão do servidor xRDP é compatível no artigo relevante.

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 7	Windows 10/11	Windows Server 2016/2019/2022	ALT Linux 10 Red OS 7.3 Astra Linux CE 2.12	Astra Linux SE 1.7
Conexão com um aplicativo virtual	✓	–	✓ Observação	✓	–	–
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	–
Microfone (minitomada)	✓	–	✓	✓ Observação	✓ Observação	✓ Observação
Dispositivo de reprodução de áudio	✓	✓	✓	✓	✓ Observação	✓ Observação

Conexão usando 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.

Antes de se conectar a um desktop remoto baseado em Linux usando um servidor xRDP que não tenha a extensão Kaspersky USB Redirector instalada, primeiro descubra qual versão do servidor xRDP é compatível no artigo relevante.

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 7.3 ALT Linux 10 Astra Linux CE 2.12 Astra Linux SE 1.7
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	–
Microfone (minitomada)	✓	✓	✓
Dispositivo de reprodução de áudio	✓	✓	✓

Conexão usando o aplicativo Web Access

No aplicativo Web Access, é possível se conectar a um ambiente remoto implementado nas infraestruturas Citrix Workspace e VMware Horizon por meio da tecnologia HTML5. O navegador Chromium™ é usado para a conexão. 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		
Tokens USB	–	–
Cartões inteligentes (USB)	–	–
Unidades USB	–	–
Impressoras (USB)	–	–
Microfone (minitomada)	✓	✓
Dispositivo de reprodução de áudio	✓	✓

A versão atual do Kaspersky Thin Client no aplicativo Web Access não é compatível com a conexão com desktops remotos que executam Linux nem com aplicativos virtuais.

Novidades

O Kaspersky Thin Client versão 2.0 tem os seguintes novos recursos e melhorias:

- Conexão com desktops e aplicativos remotos implantados na infraestrutura dos Serviços de Área de Trabalho Remota da Microsoft: foi adicionada a capacidade de conexão com desktops remotos e aplicativos virtuais do Microsoft Windows via Microsoft Remote Desktop Connection Broker.
- Adicionada a capacidade de conexão com desktops virtuais implementados em uma infraestrutura Citrix Workspace ou VMware Horizon sobre HTML5.
- Redirecionamento de dispositivos de gravação e reprodução de áudio conectados ao thin client usando miniconector para o ambiente remoto.
- Redirecionamento de cartões inteligentes, unidades USB e impressoras para um desktop remoto Linux (Astra Linux CE/SE, ALT Linux, RED OS). Para redirecionar dispositivos periféricos, instale o Kaspersky USB Redirector para o servidor xRDP no SO visitante, incluindo Basis.WorkPlace.
- Adicionado suporte para o thin client Centerm F620.
- Conexão automática após uma desconexão inesperada: recurso adicional de conexão automática com um desktop remoto por RDP em caso de conexão perdida.
- Suporte expandido para sistemas operacionais visitantes: recurso adicional para conexão com desktops remotos que executam os sistemas operacionais Microsoft Windows 11 ou Microsoft Windows Server 2022.
- Redirecionamento de impressoras para um ambiente remoto: adicionada função para impressão de documentos de um sistema operacional visitante (quando conectado por RDP, incluindo infraestrutura de desktop virtual Basis.WorkPlace) em uma impressora conectada ao thin client.
- Compatibilidade com uma nova configuração do TONK TN1200: adicionada funcionalidade para permitir ao Kaspersky Thin Client a possibilidade de iniciar e operar em dispositivos TONK TN1200 com SSDs mSATA.
- Aprimoramentos de desempenho do Kaspersky Thin Client:
  - Velocidades mais altas de entrega de um desktop remoto e aplicativos virtuais ao thin client.
  - Tempos de inicialização de thin client mais curtos.
  - Velocidades mais altas quando conectado a desktops remotos por nome de domínio.
- Estabilidade aprimorada para thin clients gerenciados com o Kaspersky Security Center.
- Adicionado suporte para espanhol e português do Brasil como interface do usuário e idiomas de entrada.
- Design e texto da interface do usuário do Kaspersky Thin Client atualizados:
  - Painel de conexão redesenhado no ambiente remoto.
  - Adicionado painel de notificação interativo.

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.

Preparação para a instalação

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:
   - KTC_uboot_<número da versão>.tar.gz — pacote de inicialização.
   - Kaspersky_Thin_Client_<número da versão>.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.

Instalação do Kaspersky Thin Client

Para instalar o Kaspersky Thin Client em um thin client:

1. Insira a unidade USB inicializável preparada na porta apropriada no thin client.
2. Ative o thin client e inicialize 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 usando uma conta com privilégios root:

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

onde:

- `./hw_install.sh` — caminho para o script de instalação.
- `KTC_uboot_<número da versão>.tar.gz` — pacote de inicialização.
- `Kaspersky_Thin_Client_<número da versão>.tar.gz` — imagem de instalação.

A mensagem *Installed OK! Remove USB drive and reboot* (Instalação OK! Remova a unidade USB e reinicie) 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

Para atualizar o Kaspersky Thin Client para a versão 2.0, você deve obter um arquivo compactado contendo as atualizações do banco de dados dos especialistas da Kaspersky. Carregue o arquivo obtido no Kaspersky Security Center Web Console (aqui também referido como Web Console) e, em seguida, crie, configure e inicie uma tarefa para baixar atualizações para o repositório do Servidor de Administração do Kaspersky Security Center (aqui também referido como Servidor) na interface do Web Console.

O Kaspersky Thin Client pode ser atualizado apenas se o thin client estiver conectado ao Kaspersky Security Center.

Um Servidor de Administração do Kaspersky Security Center pode ter apenas uma tarefa de atualização ativa com uma fonte de atualização prioritária. Por esse motivo, é recomendável usar um servidor separado para gerenciar thin clients, para que você possa receber patches de segurança críticos dos servidores de atualização da Kaspersky.

Para atualizar o Kaspersky Thin Client no thin client com o uso do Kaspersky Security Center Web Console:

1. No servidor do Kaspersky Security Center, descompacte o arquivo compactado que contém os bancos de dados de atualização recebidos dos especialistas da Kaspersky.
2. Conceda a todos os usuários no sistema direitos de acesso total à pasta descompactada executando as seguintes ações:
   a. Clique com o botão direito do mouse na pasta descompactada e selecione **Propriedades**.
   b. No menu exibido, selecione a guia **Segurança** e clique em **Editar**.
   c. Na janela exibida, clique em **Adicionar**, selecione **Avançado** e, na janela exibida, clique em **Localizar agora**.
   d. Na lista exibida, selecione o grupo **Todos** e clique em **OK**, depois clique em **OK** novamente na janela exibida.
      A guia **Segurança** é exibida e o grupo **Todos** aparece na lista **Nomes de grupo ou de usuário**.
   e. Na seção **Permissões para Todos**, marque as caixas de seleção para todos os parâmetros na coluna **Permitir**.

f. Clique em **OK** e, em seguida, clique em **OK** novamente na janela exibida.

3. Inicie o Web Console e selecione a seção **Dispositivos** e, em seguida, vá para a guia **Tarefas**.

4. Se a tarefa **Baixar atualizações no repositório do Servidor de Administração** estiver disponível na lista, vá para a próxima etapa das instruções. Se não estiver disponível, adicione-o fazendo o seguinte:

   a. Na guia **Tarefas**, clique em **Adicionar**.

   b. Na janela exibida, na lista suspensa **Tipo de tarefa**, selecione **Baixar atualizações no repositório do Servidor de Administração** e clique em **Avançar**.

   c. Clique em **Concluir** para concluir a criação da tarefa.

5. Selecione a tarefa **Baixar atualizações no repositório do Servidor de Administração** e, na janela exibida, vá para a guia **Configurações do aplicativo**.

6. No grupo de configurações **Fontes de atualizações**, marque a caixa de seleção ao lado da fonte dos **Servidores de atualização da Kaspersky** e clique em **Excluir**.

7. No mesmo grupo de configurações, clique em **Adicionar** e, na lista exibida, selecione **Pasta local ou de rede** e especifique o caminho completo para a pasta com os arquivos de atualização.

8. Clique em **Salvar** para concluir a alteração da fonte de atualização.

9. Vá para a guia **Agendamento** e selecione o valor necessário na lista suspensa **Início agendado**.

   Defina as outras configurações nesta guia, se necessário.

10. Clique em **Salvar** para concluir a configuração da tarefa.

11. Na lista de tarefas, marque a caixa de seleção ao lado da tarefa **Baixar atualizações no repositório do Servidor de Administração** e clique em **Iniciar**.

    A execução da tarefa é iniciada. É possível acompanhar o andamento da tarefa na lista de tarefas, na coluna **Status**.

12. Para exibir o resultado de uma tarefa para dispositivos individuais:

    a. Na lista de tarefas, selecione **Baixar atualizações no repositório do Servidor de Administração** e, na janela exibida, vá para a guia **Resultados**.

    b. Para exibir informações detalhadas sobre a execução da tarefa em um dispositivo, marque a caixa de seleção ao lado do dispositivo desejado e clique em **Histórico do dispositivo**.

13. Após a tarefa de download da atualização ser concluída, aceite o Contrato de Licença de Usuário Final e aprove o download das atualizações para os thin clients concluindo as etapas a seguir:

    a. No Web Console, vá para **Operações → Aplicativos Kaspersky** e selecione **Atualizações contínuas** na lista suspensa.

    b. Na lista de atualizações exibida, clique em **Você deve aceitar o EULA** ao lado da atualização necessária e, na janela exibida, leia o texto do Contrato de Licença de Usuário Final.

    c. Se você concordar com os termos do contrato, aceite-o marcando a caixa de seleção **Os termos e condições deste EULA** e confirmando sua escolha. Se você não concordar com os termos do Contrato de Licença de Usuário Final e não os aceitar, não poderá baixar atualizações para thin clients.

d. Na lista de atualizações, clique no nome da atualização e na seção **Status de aprovação da atualização** exibida, selecione **Aprovado** e confirme sua escolha.

Para obter informações detalhadas sobre a aprovação de downloads de atualizações, consulte *Aprovar e recusar atualizações de software* na Ajuda on-line do Kaspersky Security Center.

A solicitação de download da atualização será aprovada.

Assim que a solicitação for aprovada, as atualizações serão baixadas nos thin clients conectados ao Kaspersky Security Center, incluindo aqueles não incluídos nos grupos de administração ou grupos de dispositivos gerenciados.

As informações detalhadas sobre como receber e instalar as atualizações em thin clients são fornecidas em um artigo separado.

Interface do Kaspersky Thin Client

A interface do Kaspersky Thin Client contém os seguintes elementos:

- Janela principal do Kaspersky Thin Client.

  Na parte central da janela principal, é possível selecionar uma opção de conexão:

  - **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 ou VMware Horizon.

  Na janela de conexão, é possível definir as configurações de conexão RDP ou as configurações de conexão Basis.WorkPlace.

- Painel de controle do Kaspersky Thin Client. Ele contém os seguintes itens:

  - — botão do menu de desligamento. Nele, é possível encerrar ou reiniciar o Kaspersky Thin Client.
  - — 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.
    - Atualizar o 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.

  - Caso o Kaspersky Thin Client seja parte de um grupo de administração e os detalhes de contato do administrador sejam especificados nas configurações gerais do grupo, os contatos do administrador do Kaspersky Security Center também serão exibidos no painel de controle.
  - Status da conexão de rede do Kaspersky Thin Client.
  - Informações sobre novas notificações do Kaspersky Thin Client. É possível visualizar as notificações recebidas.
  - Botão para alternar o idioma de entrada do teclado.
  - Data e hora do sistema.

- Painel de conexão.

  Exibido enquanto houver conexão com um ambiente remoto.

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

- Nome da conexão.
- Status da conexão.
- Botão **Desconectar do servidor**.
- Os contatos do administrador, desde que tenham sido fornecidos durante a implementação do sistema.
- Ícone de status da rede.

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

- Ícone do aplicativo.
- Data atual definida no thin client.
- A hora atual definida no thin client.
- Idioma definido no 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.
- Log de auditoria contendo os dados sobre os certificados carregados no Kaspersky Thin Client e as informações sobre as instâncias de ativação e desativação do gerenciamento de thin clients pelo Kaspersky Security Center.
- Configurações do thin client:
  - 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.
  - Monitores principal e secundário.
  - ID do monitor principal.
  - 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.
- 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, incluindo 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.
  - Caso o uso de dois monitores esteja ativado ou desativado.
- 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:
    - Caso o redirecionamento de unidades USB esteja ativado ou desativado.
    - Caso o redirecionamento de cartões inteligentes esteja ativado ou desativado.

        - Caso o redirecionamento de impressoras esteja ativado ou desativado.
        - Caso o redirecionamento dos dispositivos de reprodução de áudio esteja ativado ou desativado.
        - Caso o redirecionamento dos dispositivos de registro de áudio esteja 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:
        - Caso a suavização de fonte esteja ativada ou desativada.
        - Caso a animação do menu esteja ativada ou desativada.
        - Caso o plano de fundo da área de trabalho seja exibido.
        - Se o conteúdo da janela é mostrado ao arrastar.
        - Caso os temas do Microsoft Windows estejam ativados ou desativados.
- Configurações de rede:
    - Caso a configuração automática de rede via DHCP esteja 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 Contrato 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.

Ativação e desativação 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 no painel traseiro do dispositivo. Para começar a trabalhar com o Kaspersky Thin Client, é necessário ativar o thin client.

O Kaspersky Thin Client permite conectar um mouse, teclado e monitor ao thin client enquanto o sistema está em execução. Quando um segundo monitor for conectado, a solicitação para configurar o layout do monitor será enviada.

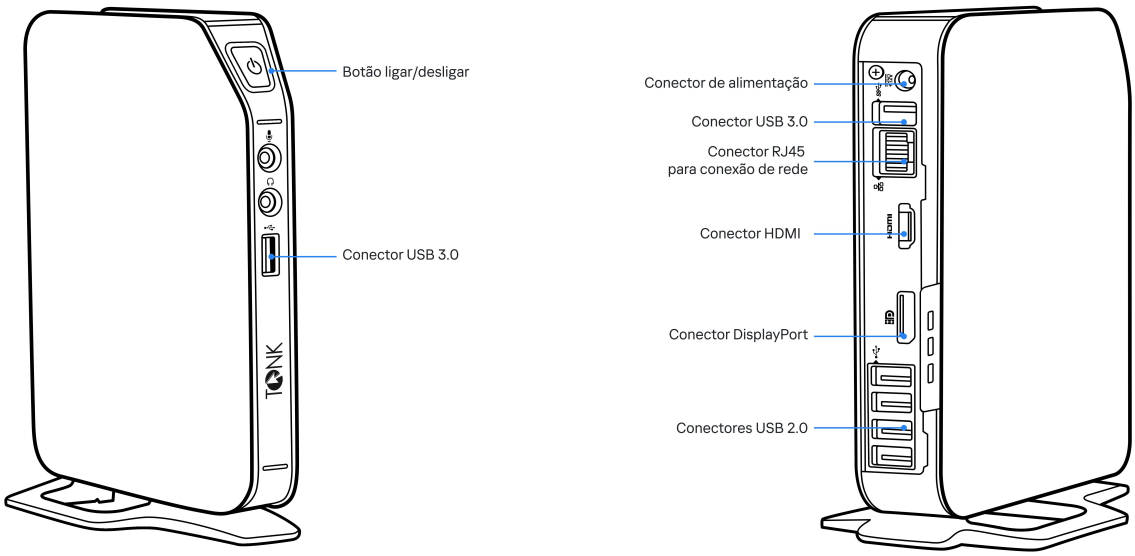
Para ativar o Kaspersky Thin Client:

Clique no botão liga/desliga na parte superior do painel frontal do thin client.

Então, o Kaspersky Thin Client começará a ser executado no thin client.

Enquanto o Kaspersky Thin Client está iniciando, o monitor conectado ao thin client exibe sequencialmente a tela inicial do fornecedor do thin client, a tela de boas-vindas do carregador de inicialização, os logs de inicialização e a tela inicial dinâmica do Kaspersky Thin Client. A aparência da janela principal do Kaspersky Thin Client na tela indica que o sistema está ligado.

Quando o Kaspersky Thin Client é iniciado pela primeira vez, a janela de aceitação do Contrato de Licença de Usuário Final é exibida. Para continuar trabalhando com o Kaspersky Thin Client, é necessário ler atenciosamente e aceitar o Contrato de Licença de Usuário Final.



Painéis frontal e traseiro do thin client TONK TN1200

Depois de terminar de trabalhar com o Kaspersky Thin Client, será necessário desativá-lo.

Para desativar o Kaspersky Thin Client,

1. Na janela principal do Kaspersky Thin Client, clique no botão de desligamento no painel de controle .

2. No menu que se abre, selecione **Encerrar**.

O Kaspersky Thin Client será desativado.

Reinicialização do Kaspersky Thin Client

É possível reiniciar o Kaspersky Thin Client caso necessário. Por exemplo, pode ser necessário reiniciar o Kaspersky Thin Client para aplicar o idioma selecionado na interface do Kaspersky Thin Client.

Para reiniciar o Kaspersky Thin Client:

1. Na janela principal do Kaspersky Thin Client, clique no botão de desligamento no painel de controle .
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.

Se um thin client não estiver conectado ao Kaspersky Security Center e o administrador não tiver atribuído certificados para ele no Web Console, um usuário poderá aceitar ou rejeitar independentemente um certificado no Kaspersky Thin Client ao conectar-se a um ambiente remoto ou a um servidor de log. 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.

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.

É recomendável 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 deve ser executada pelo administrador para configurar o Kaspersky Thin Client e o Kaspersky Security Center para estabelecer uma conexão entre eles.

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 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 seção *Instalação do Kaspersky Security Center* do guia da 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. Um arquivo comprimido contendo o pacote de distribuição do plug-in da Web está incluído no kit de distribuição.

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 detalhes sobre a ativação da porta TCP no Servidor de Administração do Kaspersky Security Center, consulte a seção *Modificar as configurações de Gerenciamento de Dispositivos Móveis* do guia da ajuda on-line do Kaspersky Security Center.

5. **Ativação do Kaspersky Thin Client**

   Ative o Kaspersky Thin Client e aguarde o carregamento 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 do Kaspersky Thin Client na lista de dispositivos gerenciados**

   Estabeleça conexão com o Kaspersky Security Center Web Console e adicione o Kaspersky Thin Client na lista de dispositivos gerenciados no Kaspersky Security Center. As políticas no Kaspersky Security Center Web Console são aplicadas apenas aos dispositivos gerenciados.

9. **Criação de uma política ativa do Kaspersky Security Center para o Kaspersky Thin Client**

   Caso precise gerenciar um grupo de dispositivos, crie uma política ativa para o Kaspersky Thin Client.

10. **Atribuição de certificados para um grupo de dispositivos**

    Atribua certificados para conectar um grupo de dispositivos 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 Kaspersky Thin Client ou pelo Kaspersky Security Center Web Console e 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 a dispositivos gerenciados**

   Na interface do Web Console, adicione um thin client ao grupo de dispositivos gerenciados se o thin client ainda estiver 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 dispositivos relevante.

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 seção *Instalação do Kaspersky Security Center* do guia da 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. Um arquivo comprimido contendo o pacote de distribuição do plug-in da Web está incluído no kit de distribuição.

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 detalhes sobre a ativação da porta TCP no Servidor de Administração do Kaspersky Security Center, consulte a seção *Modificar as configurações de Gerenciamento de Dispositivos Móveis* do guia da 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, salve-o no Servidor de Administração do Kaspersky Security Center atual como reserva e, em seguida, use-o 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

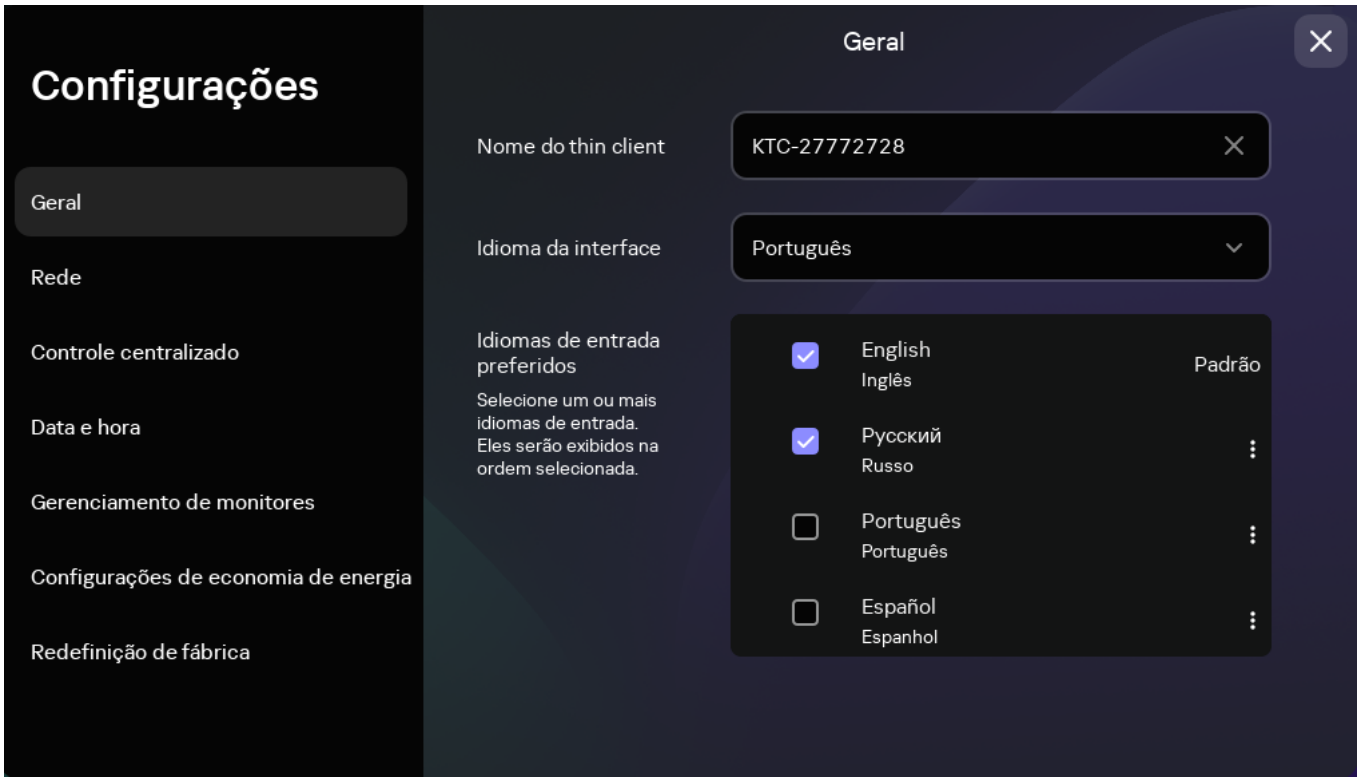
Na interface do Kaspersky Thin Client, é possível definir as configurações gerais do thin client. Por exemplo, é possível especificar o nome do thin client que será exibido na barra de tarefas do Kaspersky Thin Client e no Kaspersky Security Center Web Console, além de selecionar o idioma da interface 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 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 é compatível com os idiomas da interface do usuário em russo, inglês, espanhol e português do Brasil.

5. Na lista suspensa **Idiomas de entrada preferidos**, selecione um ou mais idiomas. O Kaspersky Thin Client é compatível com os idiomas de entrada russo, inglês, espanhol e português do Brasil. 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.

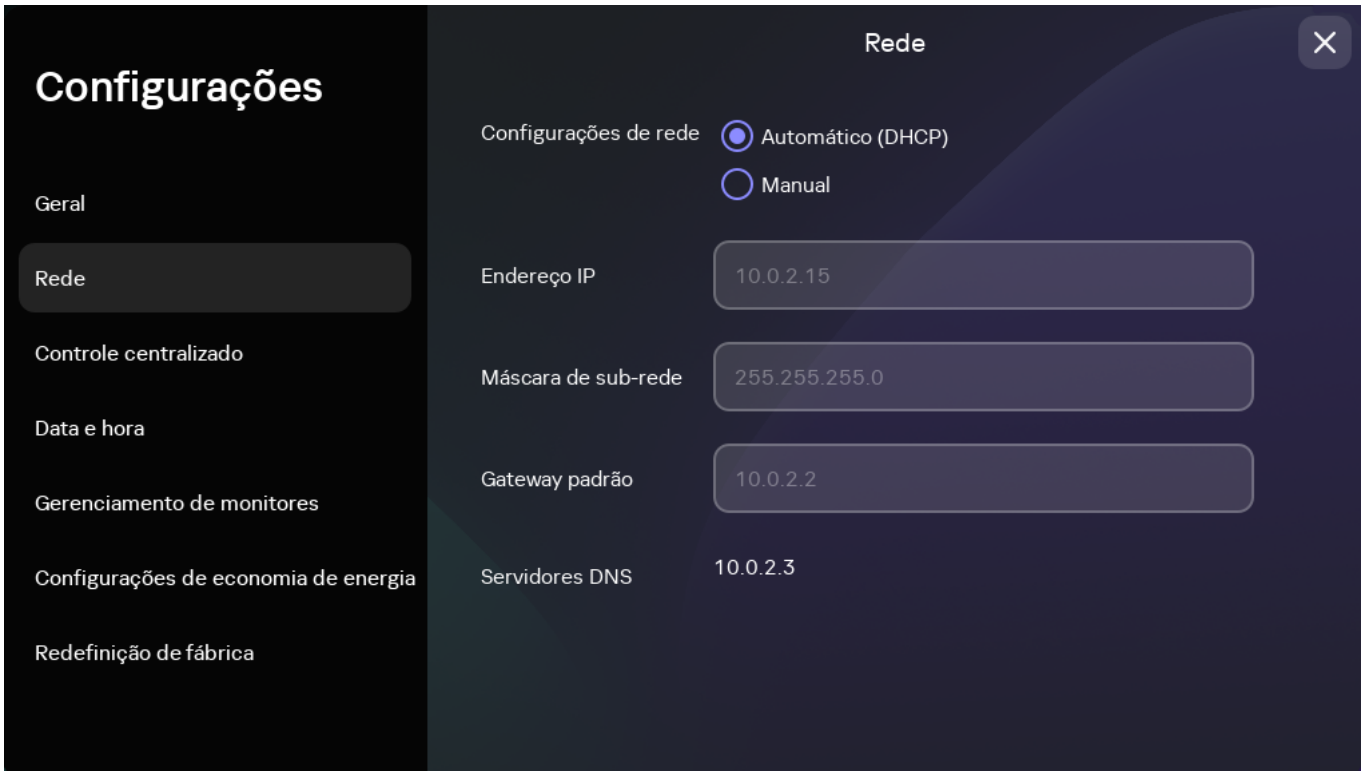
Definição das configurações de rede

Na seção **Configurações** → **Rede**, 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 **Configurações 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 **Configurações 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. Este campo é opcional.

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

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

Para controlar 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.

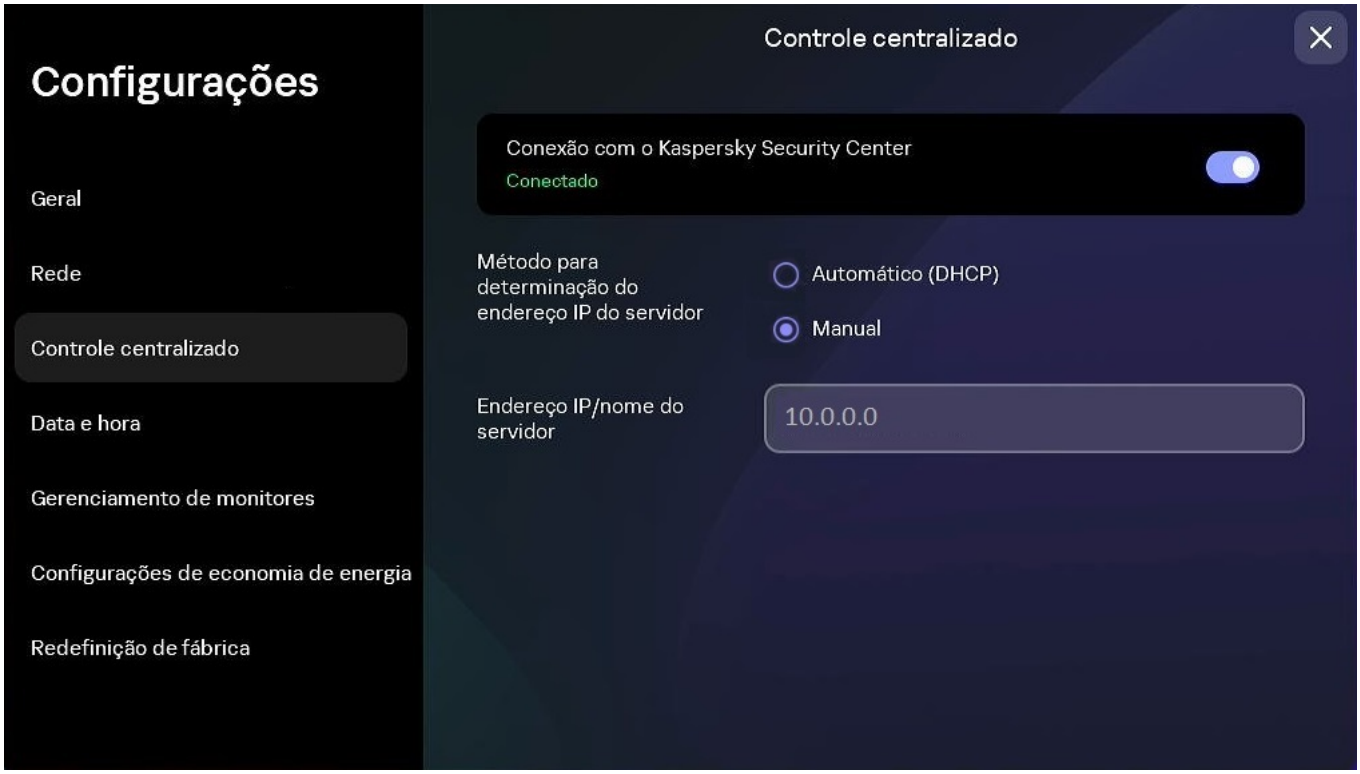
O Kaspersky Thin Client deve estar conectado ao servidor do Kaspersky Security Center em um segmento de rede seguro. Aconselhamos configurar essa conexão com a ajuda de um dos especialistas qualificados de sua empresa, que poderá verificar a autenticidade do certificado aceito.

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 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.

Definição de configurações para conexão com um ambiente remoto por RDP

O Kaspersky Thin Client possibilita definir configurações para conexão com um aplicativo virtual ou desktop remoto por RDP.

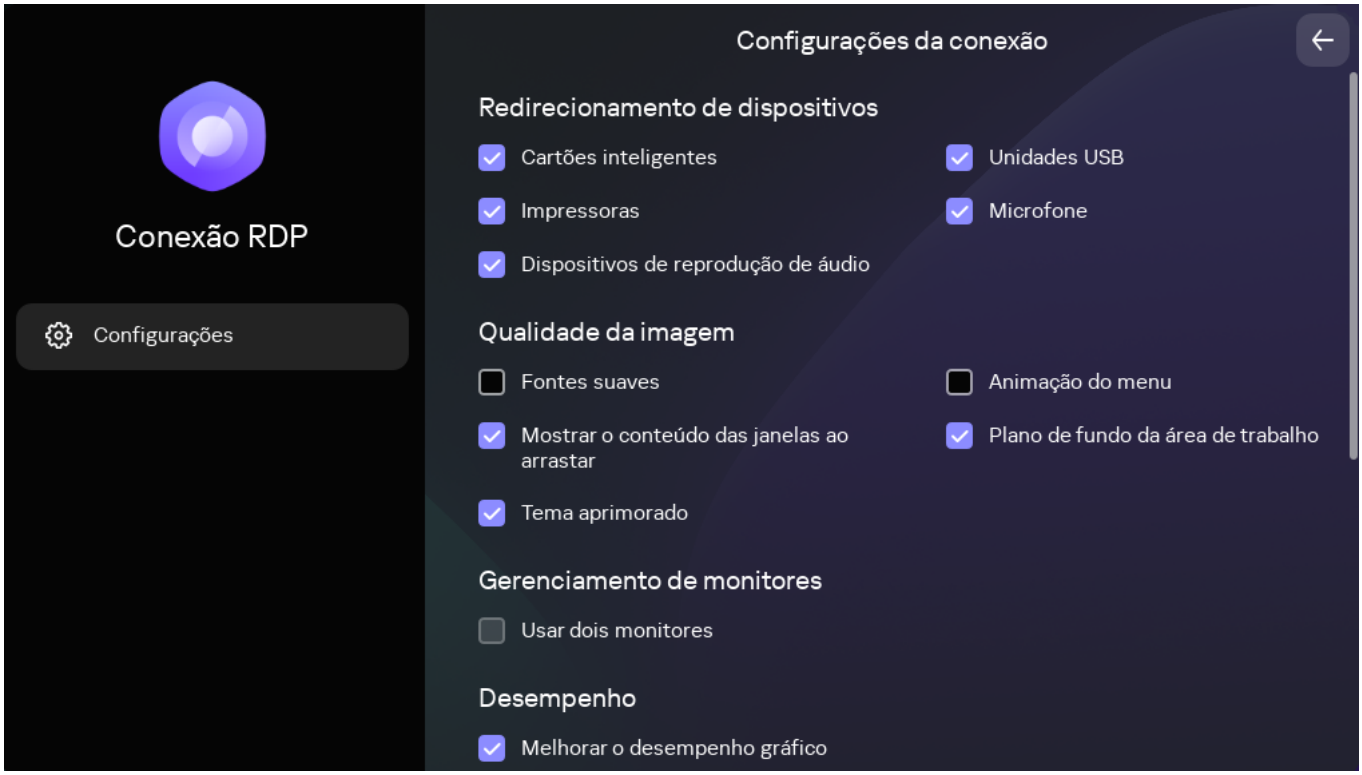
As informações sobre dispositivos que são redirecionados para um ambiente remoto são fornecidas em um artigo separado.

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 os sistemas operacionais Microsoft Windows Server 2016 e Microsoft Windows Server 2019, também é preciso permitir uma conexão remota com o uso do Remote Desktop Services e permitir que as regras de controle remoto sejam definidas para as sessões de conexão no Microsoft Remote Desktop Services.

Para definir as configurações para conexão com um desktop remoto ou aplicativo virtual por RDP:

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

   Uma janela é aberta na qual é possível definir as configurações para conexão com um desktop remoto (consulte a figura abaixo).



Janela para definir as configurações para conexão com um desktop remoto por RDP

3. No bloco de configurações **Redirecionamento de dispositivos**, ao lado dos dispositivos necessários, marque as seguintes caixas de seleção:

- **Cartões inteligentes** caso queira ativar o redirecionamento de cartões inteligentes e tokens.
- **Unidades USB** caso queira ativar o redirecionamento de unidades USB.
- **Impressoras** caso queira ativar o redirecionamento de impressoras.

  O computador remoto deve ter o driver instalado da impressora conectada ao thin client.
- **Microfone** caso queira ativar o redirecionamento de dispositivos de registro de áudio.

  O volume do áudio e outras configurações são gerenciados a partir do computador remoto.
- **Dispositivos de reprodução de áudio** caso queira ativar o redirecionamento de fones de ouvido ou alto-falantes.

  O Kaspersky Thin Client é compatível com a reprodução mono e estéreo. O volume do áudio e outras configurações são gerenciados no ambiente remoto.

4. No bloco **Qualidade da imagem**, marque as caixas de seleção ao lado das configurações gráficas do desktop remoto que precisa usar:
   - **Fontes suaves**
   - **Animação do menu**
   - **Plano de fundo da área de trabalho**
   - **Mostrar o conteúdo das janelas ao arrastar**
   - **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**. Caso necessário, é possível configurar o layout dos monitores.

6. Se você precisar melhorar a exibição e garantir uma aparência mais suave dos elementos gráficos quando conectados a um ambiente remoto, marque a caixa de seleção **Melhorar o desempenho gráfico** no bloco **Desempenho**.

   Se você precisar se conectar a um desktop remoto do Microsoft Windows 7, desmarque a caixa de seleção **Melhorar o desempenho gráfico**. Este recurso não é compatível com conexões com desktops remotos do Microsoft Windows 7.

7. 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).

   Especifique um ID da coleta do Remote Desktop Connection Broker para se conectar a um aplicativo virtual.

8. 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 sessão de conexão.

Definição de configurações para conexão com um ambiente remoto usando a infraestrutura Basis.WorkPlace

O Kaspersky Thin Client possibilita definir as configurações para conexão com um ambiente remoto usando a infraestrutura Basis.WorkPlace.

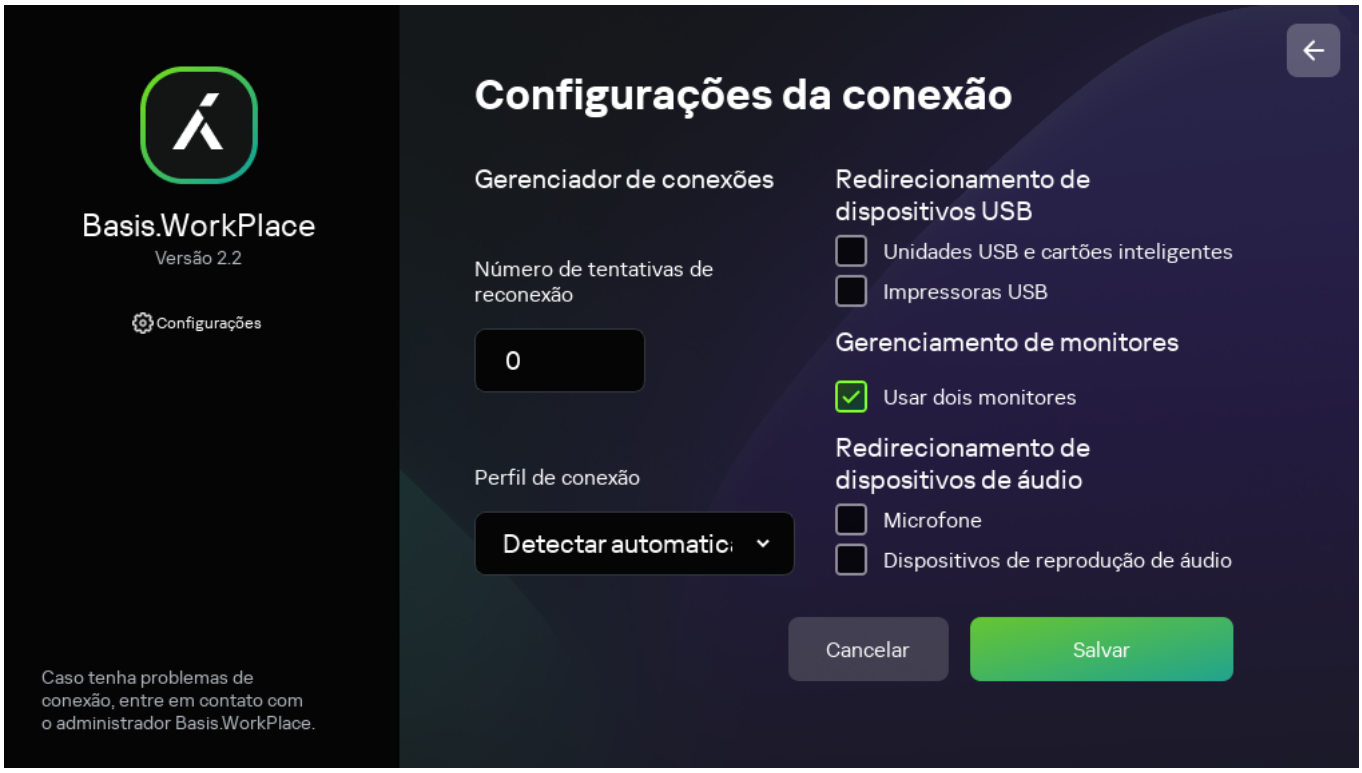
As informações sobre dispositivos que são redirecionados para um ambiente remoto são fornecidas em um artigo separado.

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

1. Na janela principal do Kaspersky Thin Client, clique no botão **Basis.WorkPlace**.

2. Na janela de conexão aberta do desktop remoto, clique em **Configurações** na parte esquerda.

   Uma janela é aberta na qual é possível definir as configurações para conexão com um desktop remoto (consulte a figura abaixo).



Janela para definir as configurações para conexão com um desktop remoto pelo Basis.WorkPlace

3. Caso seja necessário ativar ou desativar o redirecionamento de dispositivos para um ambiente remoto, marque ou desmarque as caixas de seleção apropriadas no bloco **Redirecionamento de dispositivos USB**.

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

4. 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.

5. 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**

6. 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**. Caso necessário, é possível configurar o layout dos monitores.

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

8. Clique na seta para voltar no canto superior direito da janela para retornar à janela de conexão do desktop remoto.

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.

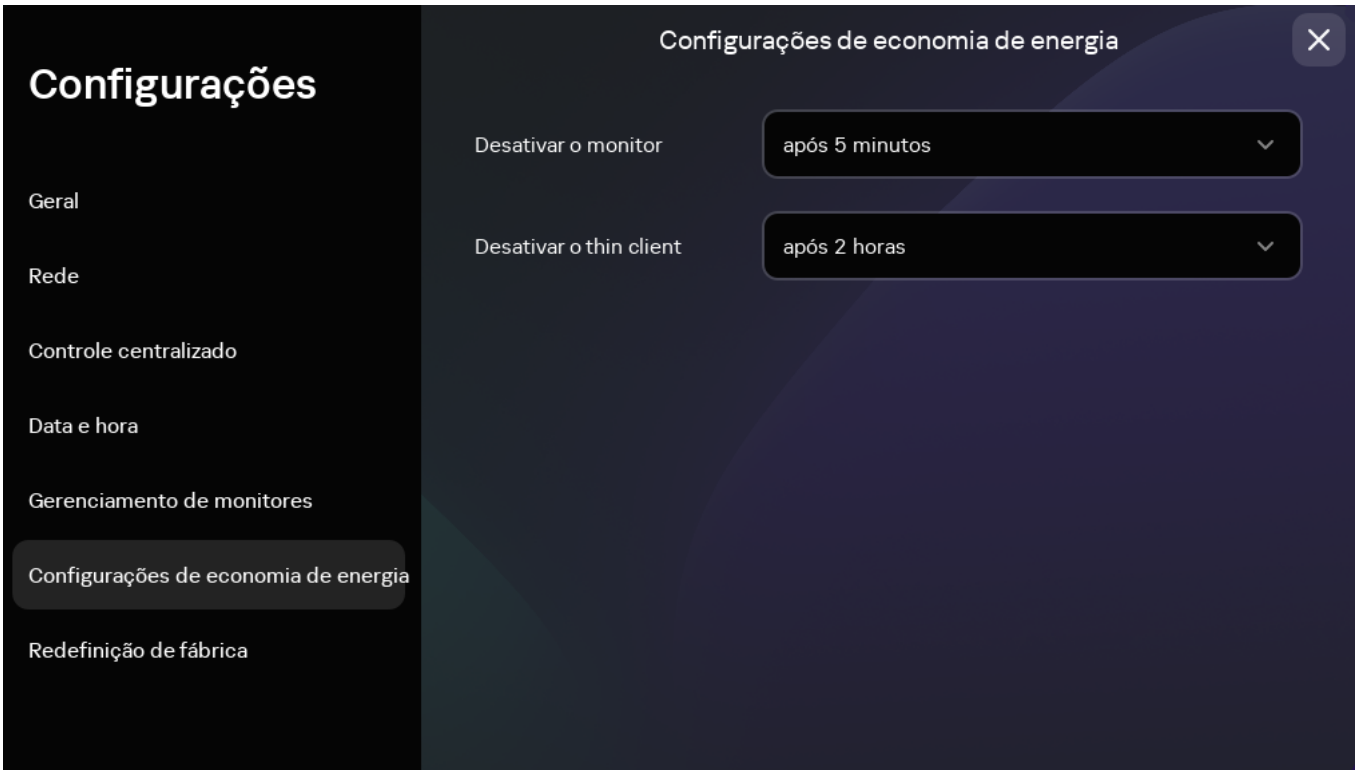
As configurações especificadas neste artigo podem estar ocultas no thin client.

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 **Configurações de economia de energia** (consulte a figura abaixo).



Configurações. Seção **Configurações de 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 pela interface do Kaspersky Security Center Web Console.

Configuração do layout de monitores

Se dois monitores estiverem instalados em sua estação de trabalho, é possível selecionar qual monitor será usado como monitor principal e qual será usado como monitor secundário ao exibir a tela do desktop remoto. Quando conectado ao desktop remoto, o painel de conexão é exibido na parte superior da tela do monitor principal.

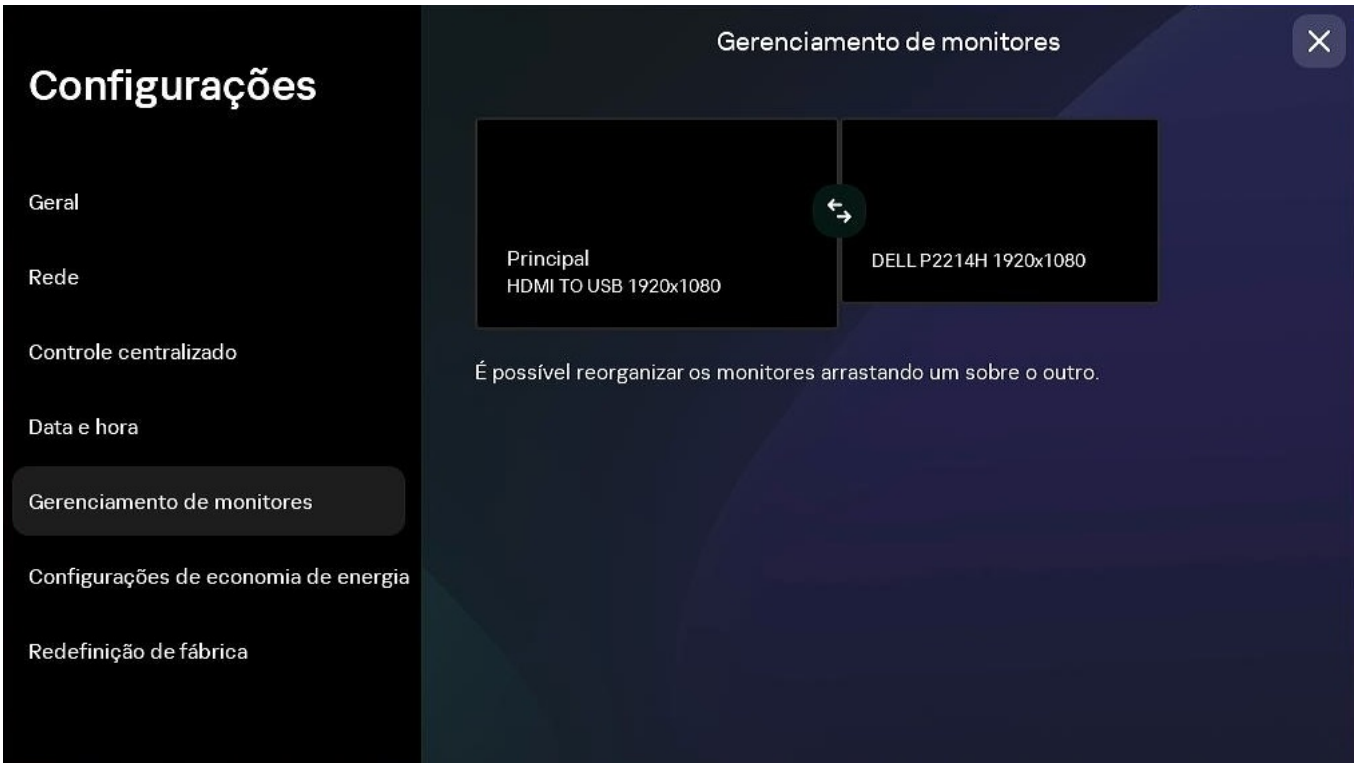
Para usar dois monitores, primeiramente é necessário ativar o suporte a monitores duplos nas configurações de conexão com desktops remotos por RDP ou gerenciados pelo Basis.WorkPlace.

Para alterar o layout de monitores para exibir o desktop remoto:

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).

   A janela aberta exibe o layout dos monitores esquematicamente. O monitor principal é sempre posicionado e rotulado à esquerda.



Configurações. Seção **Gerenciamento de monitores**

3. Altere a posição dos monitores clicando no botão localizado entre os monitores no layout.

   O layout dos monitores para exibir o desktop remoto será alterado.

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.

Se o thin client estiver incluído em um grupo de administração, os valores das configurações poderão ser aplicados pelo 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:

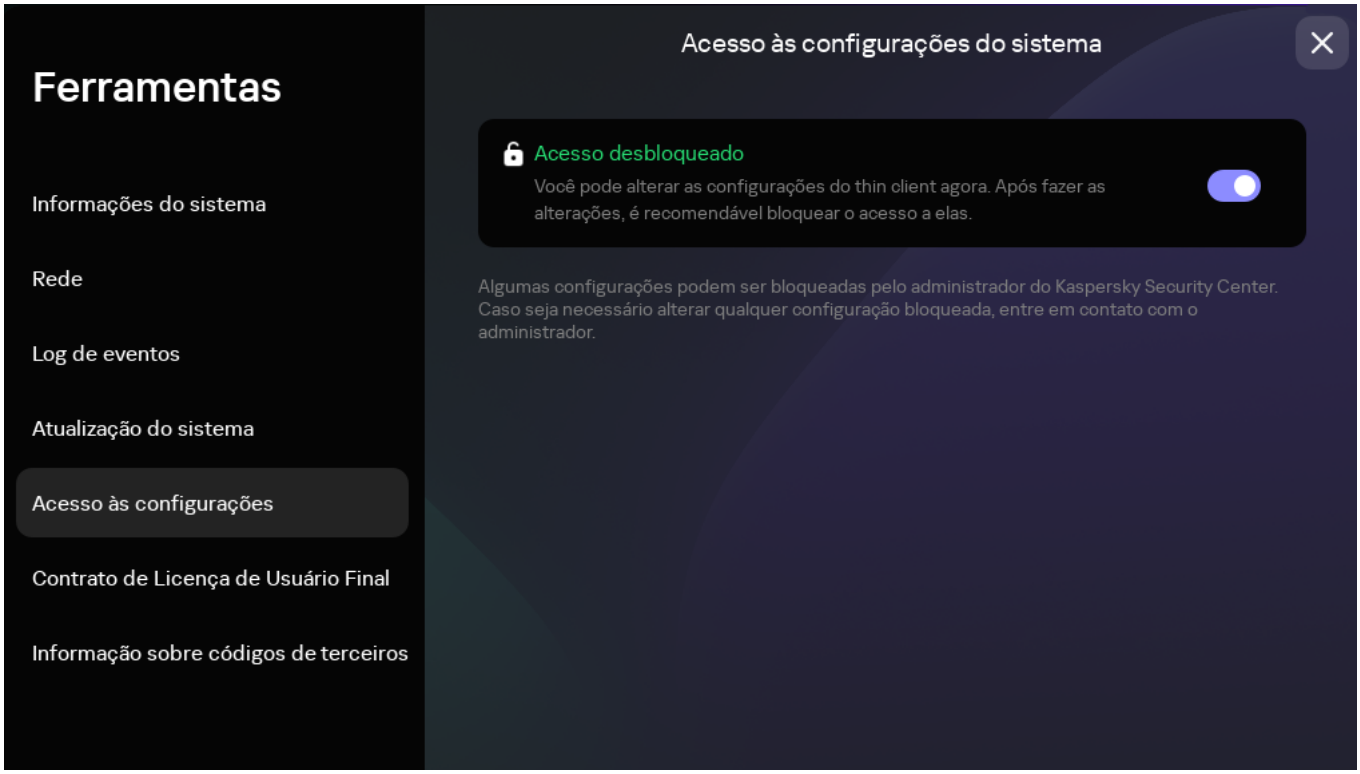
1. No painel de controle do Kaspersky Thin Client, clique em e selecione **Ferramentas** no menu aberto.
2. Na janela aberta, selecione a seção **Acesso às configurações** (consulte a figura abaixo) e execute uma das seguintes ações:
   - Caso precise ocultar as configurações, mova o botão de alternância 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 desbloqueado**.

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



Ferramentas. Seção **Acesso às configurações**

Configuração da data e a hora

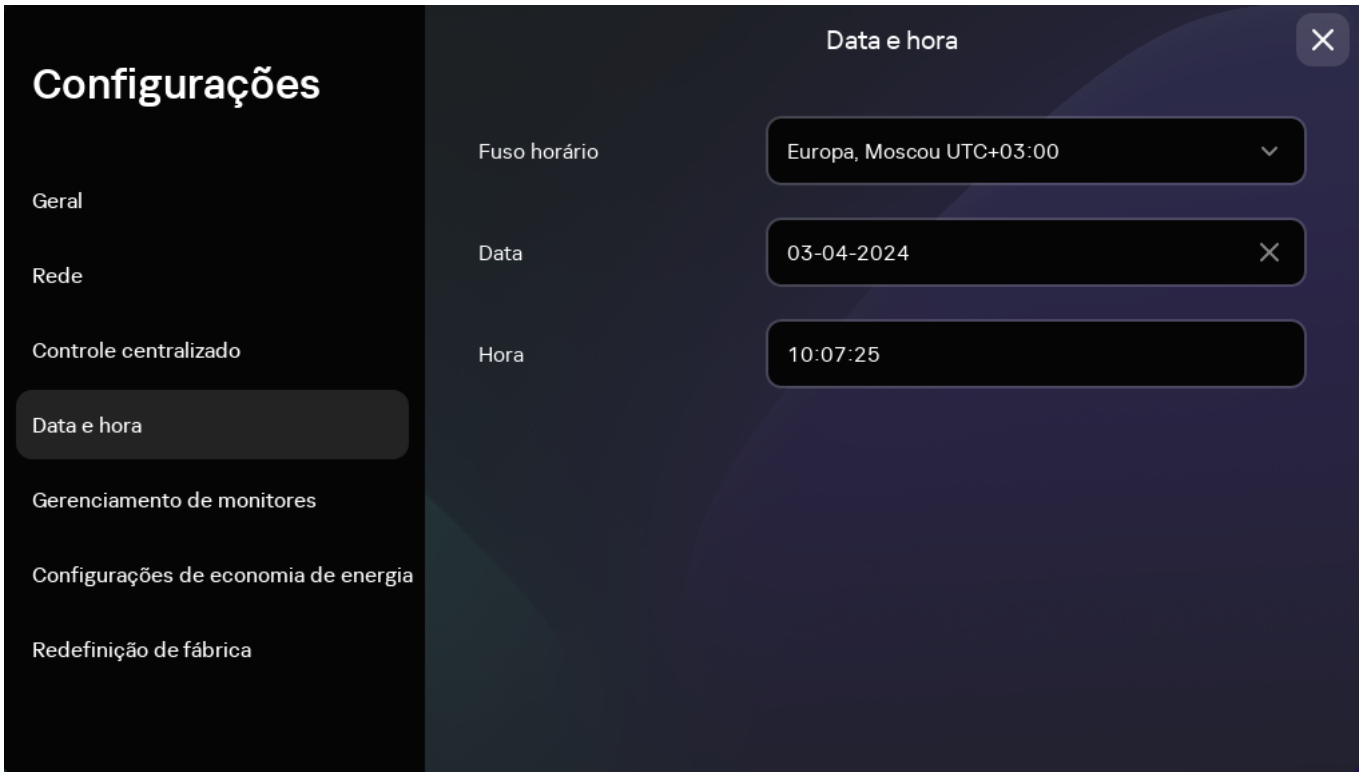
Quando um thin client está conectado ao Kaspersky Security Center, ele recebe a data e hora do Servidor de Administração do Kaspersky Security Center. É possível alterar manualmente a data e hora do Kaspersky Thin Client apenas se o sistema não estiver sendo controlado pelo Kaspersky Security Center.

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 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.

Redefinição das configurações do Kaspersky Thin Client

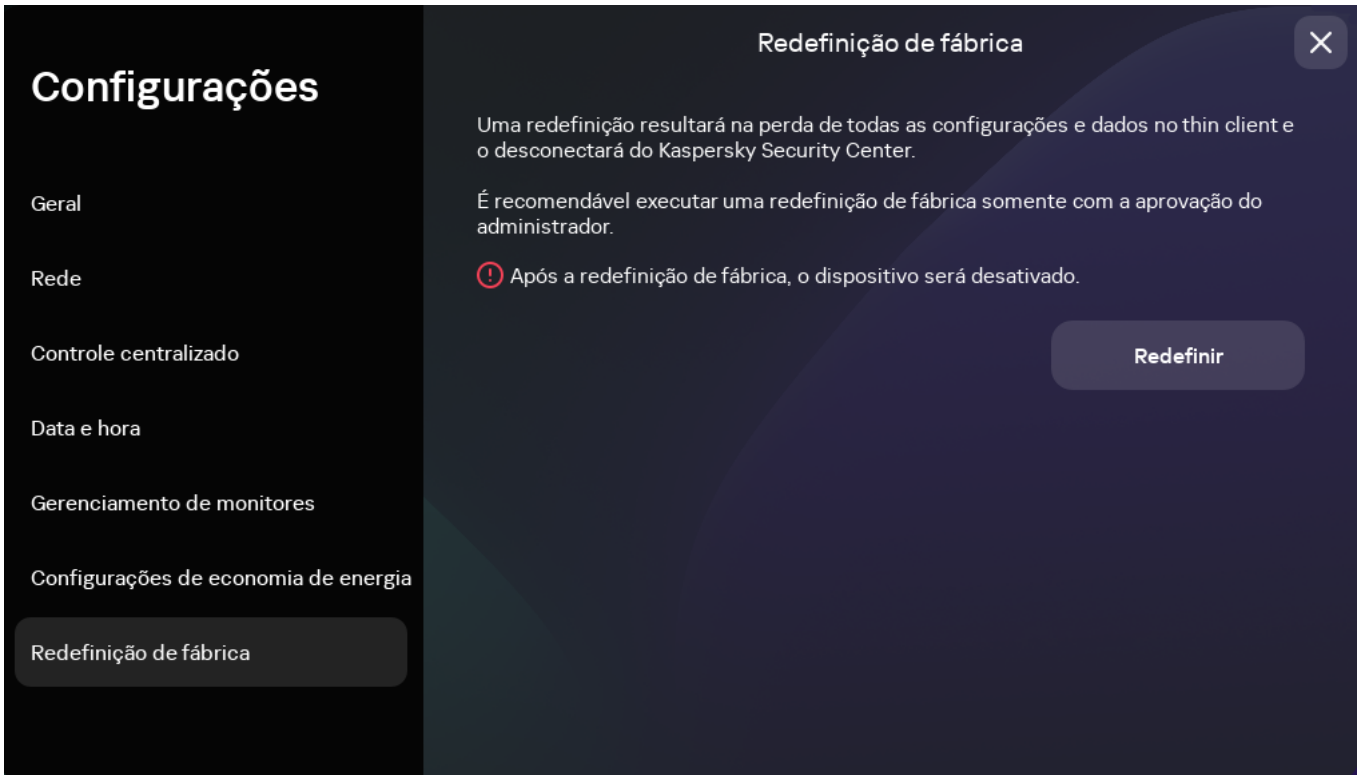
A redefinição resultará na perda de todas as configurações definidas e de todos os dados do Kaspersky Thin Client (exceto o log de auditoria e a data do sistema) e desconectará o dispositivo do Kaspersky Security Center. Recomendamos executar a redefinição somente após a aprovação do administrador de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

Para executar uma redefinição de fábrica de um thin client que não está 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** (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.

Gerenciamento do Kaspersky Thin Client na interface do thin client

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

O cenário de operação principal do Kaspersky Thin Client consiste nas seguintes etapas:

1. **Preparo do Kaspersky Thin Client para inicialização**

   Conecte os periféricos com o thin client antes de iniciá-lo pela primeira vez.

2. **Iniciação do Kaspersky Thin Client**

   Ative o thin client para começar.

3. **Sessão de conexão**

   Conecte-se com um ambiente remoto e comece a trabalhar.

4. **Bloqueio do desktop e retomada das operações**

   Caso precise sair temporariamente da sua estação de trabalho, bloqueie o desktop remoto. Retome as operações ao retornar para sua estação de trabalho. Para obter informações detalhadas sobre o bloqueio do desktop remoto e a retomada das operações, consulte o manual do sistema operacional ao qual a conexão remota está sendo estabelecida.

5. **Encerramento de uma sessão de conexão**

   Encerre a conexão com o ambiente remoto antes de desligar.

6. **Interrupção do Kaspersky Thin Client**

   Desative o thin client no final do dia de trabalho.

Conexão com um ambiente remoto

É possível usar o Kaspersky Thin Client para fazer o seguinte:

- **Conexão com um desktop remoto por RDP**

Para se conectar a um desktop remoto por RDP:

1. Ativar o Kaspersky Thin Client.
2. Na janela principal 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.

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

   Caso esteja se conectando com um desktop remoto pela primeira vez e o Kaspersky Thin Client não esteja incluído em um grupo de administração, verifique as configurações do certificado adicionado na janela aberta **Adicionar certificado** e clique no botão **Adicionar certificado**.

   Caso o Kaspersky Thin Client tenha sido adicionado anteriormente a um grupo de administração gerenciado pelo Kaspersky Security Center Web Console e o administrador do Kaspersky Security Center tenha adicionado um certificado de autenticação do servidor para o grupo de administração, a conexão será estabelecida automaticamente.

   O certificado de autenticação do servidor será adicionado no 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.

   A janela do desktop remoto é aberta e a sessão de conexão é iniciada.

- **Conexão com um aplicativo virtual via RDP**

Para se conectar a um aplicativo virtual via RDP:

1. Ativar o Kaspersky Thin Client.
2. Na janela principal 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.

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

   Caso esteja se conectando ao aplicativo virtual selecionado pela primeira vez e o Kaspersky Thin Client não esteja incluído em um grupo de administração, verifique as configurações do certificado adicionado na janela aberta **Adicionar 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.

   Caso o administrador do Kaspersky Security Center já tenha adicionado o Kaspersky Thin Client em um grupo de administração e tenha adicionado um certificado de autenticação de servidor para esse grupo, a conexão será estabelecida automaticamente.

   A janela do aplicativo virtual em execução é aberta e a sessão de conexão é iniciada.

Para alternar para outra janela de um aplicativo virtual em execução:

Passe 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 desktop remoto gerenciado pelo Basis.WorkPlace

Para se conectar a um desktop remoto gerenciado pelo Basis.WorkPlace:

1. Ativar o Kaspersky Thin Client.
2. Na janela principal 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 do gerenciador de conexões Basis.WorkPlace.

      O Kaspersky Thin Client salva o endereço do gerenciador de conexões 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 remoto. O número permitido de tentativas de entrada de senha é definido pela política de segurança ativa definida pelo administrador do Basis.WorkPlace.

4. Clique no botão **Conectar**.

   Caso esteja se conectando com um desktop remoto gerenciado pelo Basis.WorkPlace pela primeira vez, e o Kaspersky Thin Client não esteja incluído em um grupo de administração, verifique as configurações do certificado adicionado na janela aberta **Adicionar certificado** e clique no botão **Adicionar certificado**.

   Caso o Kaspersky Thin Client tenha sido adicionado anteriormente em um grupo de administração gerenciado por meio do Kaspersky Security Center Web Console, e o administrador do Kaspersky Security Center tenha adicionado um certificado para autenticar o broker Basis.WorkPlace para esse grupo de administração, a conexão com um desktop remoto gerenciado pelo Basis.WorkPlace é estabelecida automaticamente.

   O certificado para autenticar o broker Basis.WorkPlace será adicionado ao armazenamento de certificados do sistema do Kaspersky Thin Client e será usado nas conexões subsequentes.

   Uma janela para selecionar um desktop remoto será aberta e todos os desktops disponíveis para conexão serão exibidos.

5. Caso seja necessário atualizar a lista de desktops, clique no botão **Recarregar**.
6. Clique no botão com o nome do desktop ao qual deseja se conectar.

Após alguns segundos, o monitor exibirá o desktop remoto com o qual o usuário está conectado.

Na janela para conexão com os desktops gerenciados pelo Basis.WorkPlace, também é possível definir as configurações de conexão clicando em **Configurações**.

O administrador do Basis.WorkPlace pode restringir o acesso com desktops gerenciados pelo Basis.WorkPlace. Por exemplo, o administrador pode bloquear a conta de usuário ou bloquear o acesso com desktops remotos gerenciados pelo Basis.WorkPlace que estavam anteriormente disponíveis para sua conta de usuário. Caso encontre algum problema para se conectar com um desktop remoto, recomendamos entrar em contato com o administrador do Basis.WorkPlace.

- Conexão com um ambiente remoto no aplicativo Web Access

No aplicativo Web Access, é possível se conectar a um ambiente remoto implementado nas infraestruturas Citrix Workspace e VMware Horizon por meio da tecnologia HTML5. O navegador Chromium™ é usado para a conexão.

Para se conectar a um ambiente remoto no aplicativo Web Access:

1. Ativar o Kaspersky Thin Client.
2. Na janela principal do Kaspersky Thin Client, clique em **Web Access**.
3. Na janela de conexão exibida, forneça o endereço do servidor do ambiente remoto necessário no campo **Servidor**.
4. Clique no botão **Conectar**.

   Caso esteja se conectando com um ambiente remoto pela primeira vez e o Kaspersky Thin Client não esteja incluído em um grupo de administração, verifique as configurações do certificado adicionado na janela aberta **Adicionar certificado** e clique no botão **Adicionar certificado**.

   Se o Kaspersky Thin Client tiver sido adicionado anteriormente a um grupo de administração gerenciado pelo Kaspersky Security Center Web Console e o administrador do Kaspersky Security Center tiver adicionado um certificado para autenticar o endereço da Web do servidor para esse grupo de administração, a conexão com o ambiente remoto será estabelecida automaticamente.

   O certificado para autenticar o endereço do servidor Web será adicionado ao armazenamento de certificados do sistema do Kaspersky Thin Client e será usado para conexões futuras.

   Caso haja apenas um desktop remoto para o qual seja possível se conectar, seu monitor exibirá o desktop remoto para o qual o usuário está conectado. Caso haja vários desktops remotos para os quais o usuário possa se conectar, uma janela de seleção será aberta com a exibição de todos os desktops remotos disponíveis para conexão.

   Os dados necessários para usar o serviço remoto, incluindo cookies, serão armazenados no thin client até o encerramento da conexão remota. Depois disso, os dados serão excluídos.

5. Caso seja necessário atualizar a lista de desktops remotos, clique no botão **Recarregar**.
6. Clique no botão com o nome do desktop remoto ao qual deseja se conectar.

Após alguns segundos, o monitor exibirá o desktop remoto com o qual o usuário está conectado.

Múltiplas sessões de conexão em execução simultânea não são compatíveis.

O Kaspersky Thin Client usa a criptografia TLS para proteger todas as sessões de conexão e impedir que os dados sejam interceptados ou substituídos.

Uso do painel de conexão

O painel de conexão é exibido na parte superior da tela depois da conexão bem-sucedida a um ambiente remoto, e ele é usado para gerenciar a sessão de conexão ativa.

Para gerenciar uma sessão de conexão remota com a ajuda do painel de conexão, faça o seguinte:

1. Para encerrar a sessão de conexão remota, clique em **Desconectar do servidor**.
2. Para alterar o idioma da interface do thin client, clique no nome abreviado do idioma atual e selecione o idioma pertinente na lista suspensa.
3. Para visualizar as informações de Suporte Técnico, clique em .

O painel de conexão será recolhido automaticamente quando estiver fora do foco do teclado ou do mouse.

Para alternar para outra janela de um aplicativo virtual em execução:

Clique no ícone do aplicativo no painel de conexão e selecione a janela relevante na lista suspensa.

Para recolher ou restaurar o painel de conexão, faça o seguinte:

1. Para restaurar o painel de conexão, clique no painel recolhido ou pressione **`Ctrl+Alt+Home`**.
2. Para recolher o painel de conexão com o foco do teclado, pressione **`Esc`**.
3. Para recolher o painel de conexão sem mover o foco para fora da janela da sessão remota, pressione **`Ctrl+Alt+Home`**.

Também é possível mover um painel de conexão recolhido horizontalmente para a direita ou para a esquerda.

Para alterar a posição do painel de conexão:

Clique na área do painel de conexão que não tem botões e arraste-a com o mouse.

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

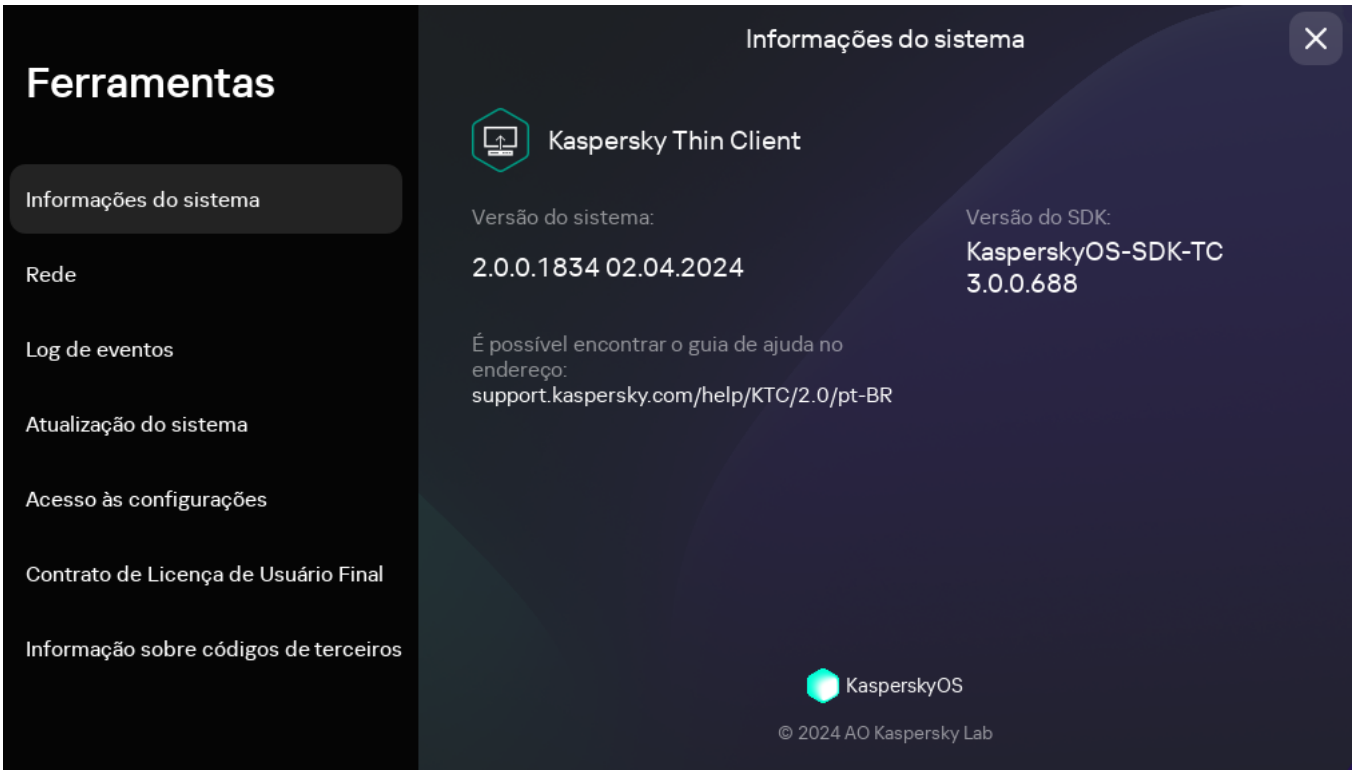
Também é possível controlar o painel de conexão e a sessão remota com teclas de atalho.

Exibição das informações sobre o Kaspersky Thin Client

É possível visualizar as informações sobre o Kaspersky Thin Client em **Ferramentas** → **Informações do sistema**.

A seção **Informações do sistema** (consulte a figura abaixo) exibe os seguintes dados:

- Número da versão do Kaspersky Thin Client
- Número da versão do KasperskyOS
- Link para a ajuda on-line do Kaspersky Thin Client



Ferramentas. Seção de **Informações do sistema**

Exibição das informações do status da rede

É possível visualizar as configurações de conexão de rede do Kaspersky Thin Client e o status da rede em **Ferramentas** → **Rede**. As informações sobre as configurações de conexão de rede do Kaspersky Thin Client são atualizadas automaticamente pelo menos uma vez a cada segundo.

A seção **Rede** exibe as seguintes informações sobre as configurações para conectar o Kaspersky Thin Client na rede (consulte 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.

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.
- Uma solicitação 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.

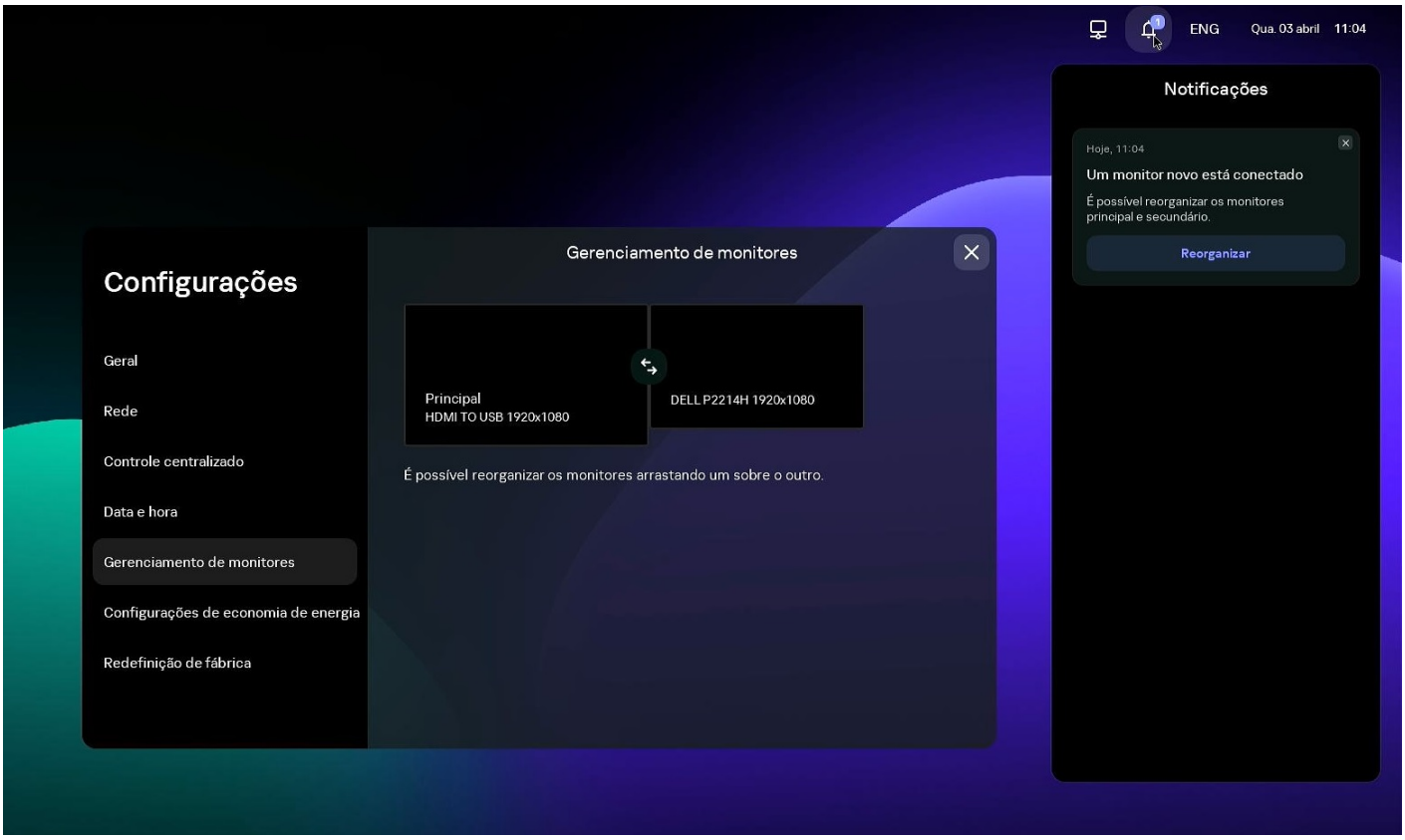
Caso o foco do cursor ou do teclado esteja fora da área de notificação, as solicitações não resolvidas e não lidas serão ocultadas, e o contador no painel de controle exibirá seu número.

Durante uma sessão de conexão, as notificações de atualização não são ocultadas automaticamente. É possível fechar manualmente essas notificações ou selecionar a ação pertinente para fechar uma notificação.

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

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

Uma lista de notificações será exibida se houver novas notificações disponíveis (veja a figura abaixo).



Painel de notificações do Kaspersky Thin Client

Gerenciamento de certificados na interface do 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 thin clients a um servidor de log e a um ambiente remoto usando somente certificados que foram 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.

Encerramento de uma sessão de conexão

Para encerrar uma sessão de conexão remota:

Restaure o painel de conexão e clique em **Desconectar do servidor** no painel.

A sessão é fechada e uma janela de conexão é exibida.

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

É possível usar teclas de atalho dedicadas e combinações de teclas ao trabalhar com o Kaspersky Thin Client e durante a sessão de conexão. 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 as opções de conexão disponíveis (**RDP**, **Basis.WorkPlace**, **Web Access**)

←	na janela principal do Kaspersky Thin Client.
↑ ↓	• Alterna entre os itens da lista suspensa. • Rola o conteúdo da página para cima ou para baixo.
Tab	Alterna da *esquerda* para a *direita* ou de *cima* para *baixo* 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 *direita* para a *esquerda* ou de *baixo* para *cima* 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 uma sessão de conexão. O atalho só funciona em um painel de conexão expandido.
Win+I	Abra **Configurações** na janela principal do Kaspersky Thin Client se o acesso às configurações estiver desbloqueado.
Win+U	Abre **Ferramentas** na janela principal do Kaspersky Thin Client.
Win+Esc	Encerra o Kaspersky Thin Client na janela principal do Kaspersky Thin Client.
Win+F12 ou	Reinicia o Kaspersky Thin Client na janela principal do Kaspersky Thin Client.

Win+End	
Win+A or **Win+N**	Abre o painel de notificações na janela principal do Kaspersky Thin Client.
Win+↓ **Win+↑**	Recolhe ou restaura uma janela enquanto estiver conectado com um aplicativo virtual.
Win+M	Minimiza todas as janelas enquanto estiver conectado com um aplicativo virtual.
Win+Shift+M	Restaura todas as janelas enquanto estiver conectado com um aplicativo virtual.

Atualização do Kaspersky Thin Client na interface do thin client

O Kaspersky Thin Client pode ser atualizado apenas se o thin client estiver conectado ao Kaspersky Security Center.

Depois que as atualizações forem baixadas para o dispositivo, a interface do Kaspersky Thin Client exibe uma notificação com a hora em que a atualização será aplicada.

É possível instalar uma atualização em uma das seguintes maneiras:

- **Diretamente a partir da notificação sobre a atualização disponível**

  - Caso queira instalar a atualização agora, clique no botão **Reiniciar agora** na janela de notificação de atualização disponível.

    As atualizações serão instaladas e o Kaspersky Thin Client será reiniciado.

  - Caso queira instalar as atualizações posteriormente, clique em **Mais tarde** na janela de notificação de atualização disponível. A notificação de atualização exibe por quanto tempo a atualização será adiada. A hora da inicialização adiada da atualização é definida pelo administrador.

    A reinicialização e a atualização do sistema serão adiadas.

    Caso queira ignorar ou fechar a notificação de atualização do Kaspersky Thin Client diversas vezes, a atualização será instalada automaticamente.

- **Ao reiniciar ou desativar o thin client**

  1. No painel de controle do Kaspersky Thin Client, clique no botão de desligamento .
  2. Se planejar sair ou continuar trabalhando com o Kaspersky Thin Client após a atualização, execute uma das seguintes ações:

     - Caso queira continuar trabalhando, selecione **Atualizar e reiniciar** no menu aberto.

       As atualizações serão instaladas e o Kaspersky Thin Client será reiniciado.

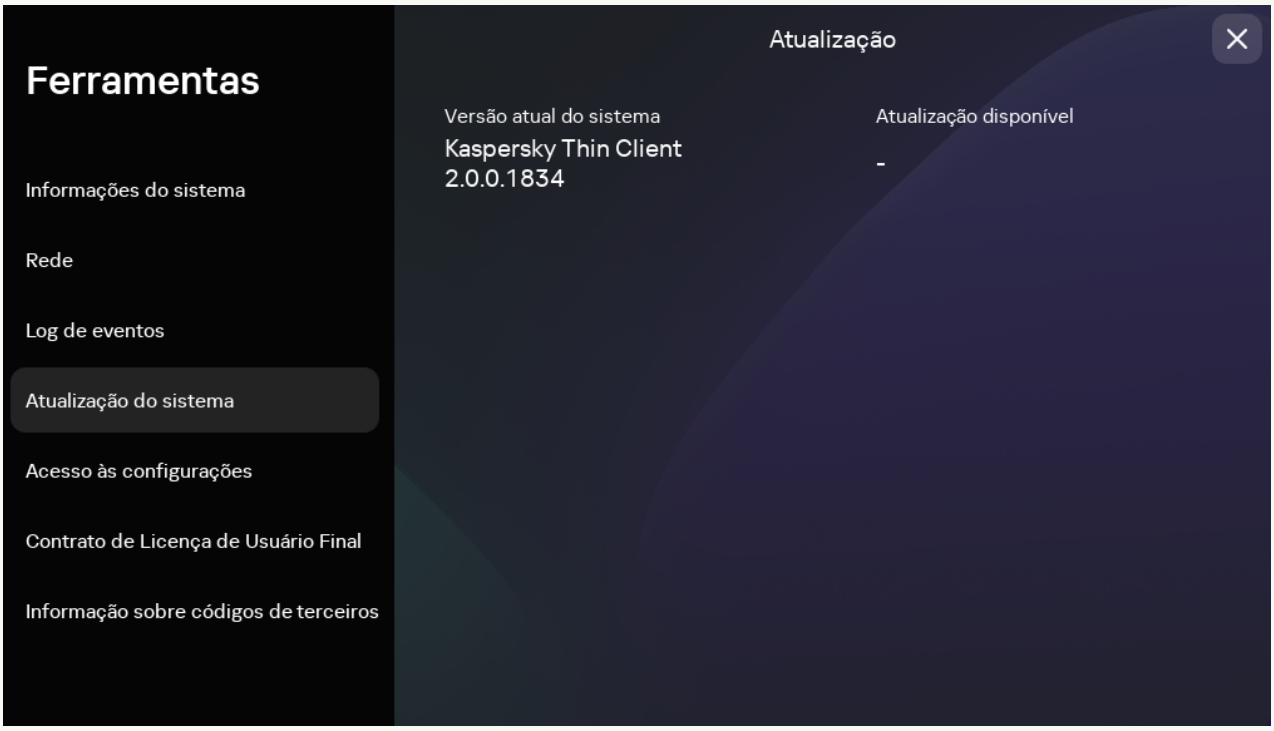
     - Caso queira parar de trabalhar, selecione **Atualizar e encerrar** no menu aberto.

       As atualizações serão instaladas e o Kaspersky Thin Client será desligado.

- Na seção Atualização do sistema

1. No painel de controle do Kaspersky Thin Client, clique em e selecione **Ferramentas** no menu aberto.
2. Selecione a seção **Atualização do sistema**.

   Uma janela é aberta, exibindo as informações sobre a versão atual do sistema e as atualizações baixadas (consulte a figura abaixo).



Ferramentas. Seção Atualização do sistema

3. Clique em **Instalar e reiniciar**. Caso não tenha nenhuma atualização disponível, o botão não será exibido.

As atualizações serão instaladas e o Kaspersky Thin Client será reiniciado.

Caso uma atualização do Kaspersky Thin Client tenha sido baixada, sem que o usuário ainda tenha reiniciado, a atualização será instalada automaticamente durante a próxima reinicialização ou desligamento do dispositivo.

Informações detalhadas sobre a atualização centralizada de thin clients com o uso do Web Console são fornecidas em um artigo separado.

Gerenciamento do Kaspersky Thin Client pelo Kaspersky Security Center Web Console

O Kaspersky Security Center Web Console (ou simplesmente, "Web Console") é um aplicativo da Web criado para permitir 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 o guia da ajuda on-line do Kaspersky Security Center Web Console.

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 está incluído no kit de distribuição do Kaspersky Thin Client e facilita a interação entre o Kaspersky Thin Client e o Kaspersky Security Center.

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

- Gerenciar as configurações do Kaspersky Thin Client.
- Receber e visualizar eventos do Kaspersky Thin Client.
- 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:

- Ao configurar o Kaspersky Thin Client, é preciso especificar as configurações para se conectar ao Kaspersky Security Center.
- No Kaspersky Security Center Web Console, é preciso instalar o plug-in da Web do Kaspersky Security Management Suite.

Instalação do plug-in da Web do 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 detalhes sobre a ativação de portas em um Servidor de Administração do Kaspersky Security Center, consulte a seção *Modificar as configurações de Gerenciamento de Dispositivos Móveis* do guia da ajuda on-line do Kaspersky Security Center.

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 de gerenciamento 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 digital (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, remova o dispositivo do grupo de Dispositivos gerenciados.

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

1. No menu da interface 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 como configurar o acesso baseado em função, consulte a *Configurar direitos de acesso aos recursos do aplicativo. Controle de acesso baseado em função* seção do guia da ajuda on-line do Kaspersky Security Center.

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

- *Diretor de segurança*. Essa função tem permissões para visualizar todas as seções do Kaspersky Security Management Suite e gerenciar os certificados do Kaspersky Thin Client. É possível atribuir essa função a um funcionário responsável pela segurança das informações em sua empresa.
- *Administrador*. Essa função tem permissões para visualizar todas as seções do Kaspersky Security Management Suite e gerenciar as configurações de conexão do desktop remoto, configurações gerais e configurações do sistema e dados do Kaspersky Thin Client. É possível atribuir essa função a um funcionário responsável pelo suporte e administração dos sistemas de informação em sua organização.
- *Administrador avançado*. Essa função tem permissões para visualizar e gerenciar todas as seções do Kaspersky Security Management Suite e gerenciar certificados, configurações de conexão do desktop remoto, configurações gerais e configurações do sistema e dados do Kaspersky Thin Client. 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 descreve as funções disponíveis para um usuário, dependendo da função atribuída para gerenciar o Kaspersky Thin Client. 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	✓	–	✓

Definir configurações para conexão com os desktops remotos 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	–	✓	✓

Fazendo login e logout do Web Console

Para efetuar login no Web Console, é necessário solicitar ao administrador o endereço da Web do Servidor de Administração do Kaspersky Security Center e o número da porta especificados durante a instalação (a porta 8080 é usada por padrão). Também é preciso ativar o JavaScript em seu navegador.

Para efetuar login no Web Console:

1. Em seu navegador, vá para `https://<endereço do Servidor de Administração>:<Número da porta>`. Para obter os requisitos do navegador do Kaspersky Security Center Web Console, consulte a seção *Requisitos de hardware e software* seção do guia da ajuda on-line do Kaspersky Security Center Web Console.

   A página de login é aberta.

2. Efetue o login usando o nome de usuário e senha de um administrador local.

   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. Caso esteja entrando no Web Console pela primeira vez, o assistente de início rápido será iniciado. Para obter informações adicionais sobre como o Kaspersky Security Center Web Console funciona, consulte o guia da ajuda on-line do Kaspersky Security Center Web Console.

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.

Adição de um thin client ao grupo de dispositivos gerenciados

No Web Console, você pode controlar centralmente os thin clients que estão conectados com o Kaspersky Security Center. Por exemplo, você pode adicioná-los a grupos de administração e aplicar as políticas necessárias. Para controlar centralmente um thin client, você deve primeiro adicioná-lo ao grupo de dispositivos gerenciados.

Para adicionar um thin client ao grupo de dispositivos gerenciados:

1. Na janela principal do Web Console, selecione **Descoberta e implementação → Dispositivos não atribuídos**.

   A lista de todos os dispositivos não atribuídos detectados será exibida.

2. Marque a caixa de seleção ao lado do nome do dispositivo que deseja adicionar ao grupo de dispositivos gerenciados.

3. Clique no botão **Migrar para grupo**.

   O painel **Migrar para grupo** é aberto à direita. Marque a caixa de seleção ao lado do grupo de administração de **Dispositivos gerenciados**.

4. Clique no botão **Migrar**.

O thin client será adicionado ao grupo de dispositivos gerenciados.

Gerenciamento de políticas

Uma *política* é um conjunto de configurações operacionais do Kaspersky Thin Client definidas para um grupo de administração. É possível configurar várias políticas com valores diferentes para um dispositivo. Para diferentes grupos de administração, as configurações do aplicativo podem ser diferentes. Cada grupo de administração pode ter a própria política para o aplicativo. Para obter informações mais detalhadas quanto ao uso das políticas do Kaspersky Security Center para gerenciar o aplicativo, consulte a seção *Políticas e perfis da política* do guia da ajuda on-line do Kaspersky Security Center.

As configurações de política são definidas no Kaspersky Security Center Web Console usando o plug-in da Web e são transmitidas para o Kaspersky Thin Client quando o aplicativo é sincronizado com o Kaspersky Security Center. O período de sincronização pode ser alterado nas configurações de política.

Política ativa e inativa

Uma política se destina a um grupo de dispositivos gerenciados e pode estar ativa ou inativa. As configurações de uma política ativa são salvas em dispositivos cliente durante a sincronização. Não é possível aplicar várias políticas simultaneamente a um dispositivo, portanto apenas uma política pode estar ativa em cada grupo.

É possível criar um número ilimitado de políticas inativas. Uma política inativa não afeta as configurações do aplicativo em dispositivos na rede. As políticas inativas tem como propósito servir de contingência durante as situações de emergência, como um ataque de vírus. Caso haja um ataque por unidades USB, é possível ativar uma política que bloqueia o acesso a elas. Nesse caso, a política ativa fica automaticamente inativa.

Herança de configurações

As políticas, como os grupos de administração, têm uma hierarquia. Por padrão, uma política secundária herda as configurações da política principal. Uma *política secundária* é uma política para níveis de hierarquia aninhados. Em outras palavras, é uma política para grupos de administração aninhados e Servidores de Administração secundários. É possível desativar a herança de configurações da política principal.

Cada configuração de política tem o atributo que indica se as configurações podem ser modificadas nas políticas ou nas configurações do aplicativo local. Dependendo do status desse atributo, um dos seguintes valores é exibido ao lado de uma configuração:

- Indefinido **Indefinido**. Caso um ícone de cadeado aberto seja exibido ao lado de uma configuração e o botão de alternância seja desativado, essa configuração não estará definida na política. Um usuário pode alterar essas configurações na interface local do aplicativo Kaspersky. Essas configurações são chamadas de desbloqueadas.

- Aplicado **Aplicado**. Caso um ícone de cadeado fechado seja exibido ao lado de uma configuração e o botão de alternância seja ativado, essa configuração será aplicada nos dispositivos aos quais a política é aplicada. Um usuário não pode alterar os valores dessas configurações na interface local do aplicativo Kaspersky. Essas configurações são denominadas bloqueadas.

O atributo se aplica a uma política secundária somente se a herança das configurações da política principal estiver ativada para a política secundária.

Criação da política

Para gerenciar um grupo de dispositivos que executam o Kaspersky Thin Client pelo Web Console, é necessário criar uma política.

Para criar uma política para um grupo de dispositivos:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Clique no botão **Adicionar**.
3. Na lista de aplicativos na janela aberta, selecione o Kaspersky Security Management Suite e clique em **Avançar**.
4. Na janela de configuração da nova política, na guia **Geral**, especifique as seguintes configurações:
   - No campo **Nome**, insira o nome da política. Por padrão, o campo exibe o nome do plug-in de gerenciamento da Web do Kaspersky Thin Client como Kaspersky Security Management Suite.
   - No bloco **Status da política**, selecione um dos seguintes status: *Ativo*, *Inativo*, *Ausência*. O status padrão é *Ativo*.
   - Caso precise definir a herança de configurações da política, defina as seguintes configurações no bloco **Herança de configurações**:
     - Ative ou desative a opção **Herdar configurações da política principal**.
     - Ativar ou desativar a opção **Forçar herança de configurações nas políticas secundárias**.
5. Clique no botão **Salvar** na parte inferior da página.

A política será criada e aparecerá na lista de políticas do Web Console.

Edição de uma política

É possível editar uma política criada anteriormente para um grupo de dispositivos que executam o Kaspersky Thin Client.

Para alterar uma política:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Políticas e perfis**.
2. Selecione a política que precisa ser editada.
3. Na janela de configuração de política aberta, defina as seguintes configurações na guia **Geral**:

- Caso seja necessário, insira um novo nome da política no campo **Nome**.
- Caso seja necessário alterar o status da política, use o bloco **Status da política** para selecionar um dos seguintes status: *Ativo*, *Inativo*, *Ausência*.
- Caso precise definir a herança de configurações da política, defina as seguintes configurações no bloco **Herança de configurações**:
  - Ative ou desative a opção **Herdar configurações da política principal**.
  - Ativar ou desativar a opção **Forçar herança de configurações nas políticas secundárias**.

4. Clique no botão **Salvar** na parte inferior da página.

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

Definição das configurações do Kaspersky Thin Client pelo Web Console

Esta seção contém informações quanto à definição das configurações do Kaspersky Thin Client pelo Web Console.

Definição de configurações básicas do Kaspersky Thin Client pelo Web Console

No Web Console, é possível definir as configurações gerais para um dispositivo ou um grupo de dispositivos que executam o Kaspersky Thin Client.

Como definir as configurações básicas para um dispositivo

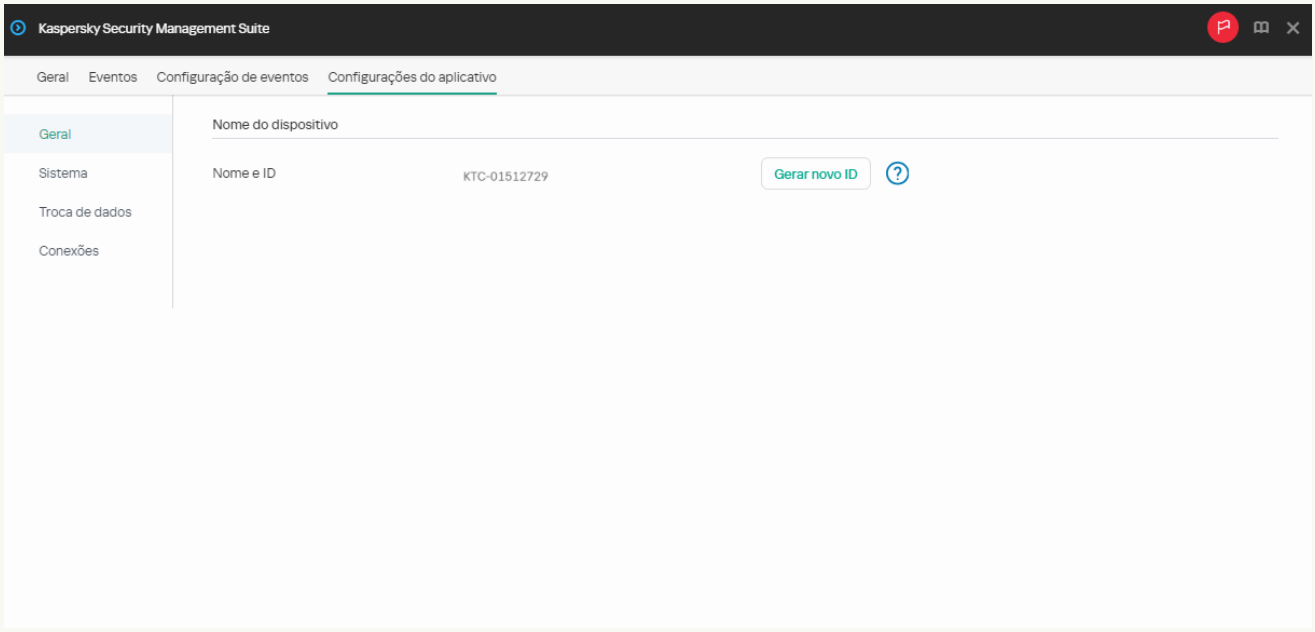
1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do thin client onde o Kaspersky Thin Client está em execução. É possível visualizar o nome do dispositivo na interface do Kaspersky Thin Client. Caso o nome do thin client não esteja na lista, adicione-o ao grupo **Dispositivos gerenciados**.

   Caso um dispositivo gerenciado seja adicionado a um grupo de administração e uma política aplicada seja definida para as configurações desse grupo, as configurações definidas individualmente para o dispositivo não serão aplicadas.

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



Janela para definir as configurações gerais pelo Web Console para um dispositivo

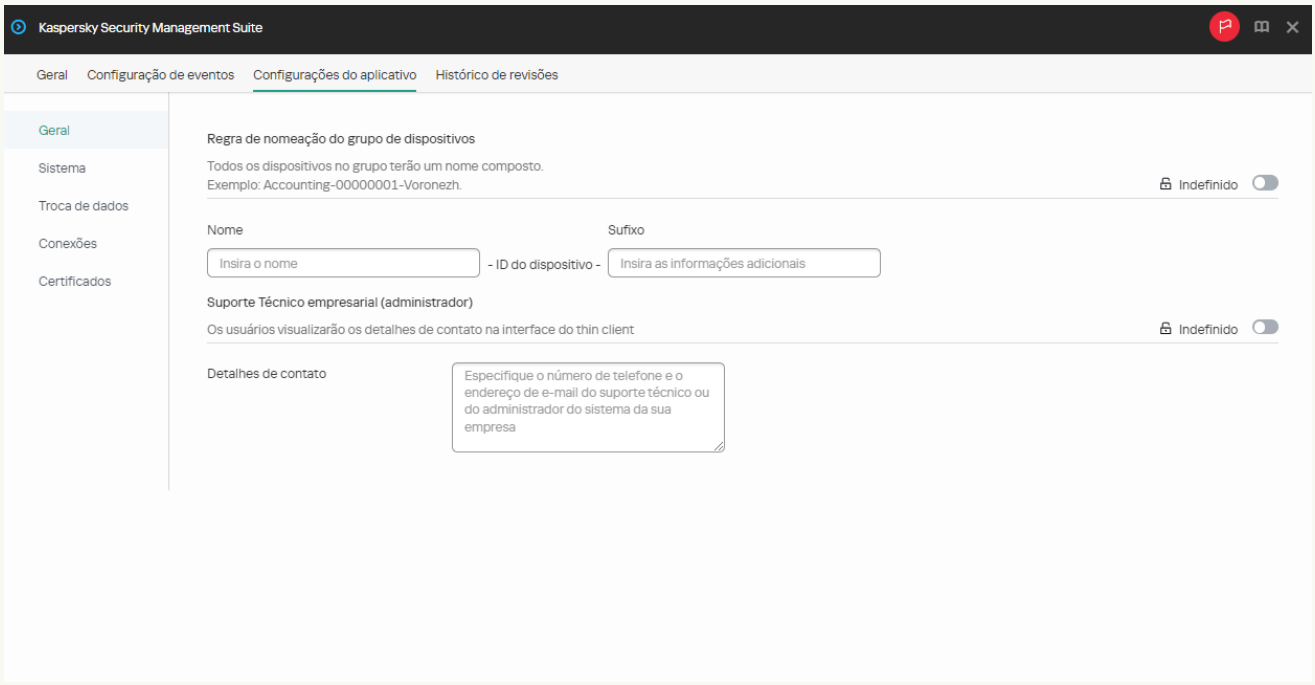
7. Caso seja necessário alterar o ID no nome do thin client, clique no botão **Gerar novo ID** no bloco **Nome do dispositivo**. O dispositivo gerenciado para o qual o usuário deseja gerar um novo ID deve ser adicionado a um grupo de administração, e esse grupo deve ter uma política configurada e aplicada para uma regra de nomeação do grupo de dispositivos.

   O novo ID no nome do thin client será criado após o dispositivo ser sincronizado com o Kaspersky Security Center.

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

Como definir as configurações básicas para um grupo de dispositivos

1. Na janela principal do Web Console, selecione **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).



Janela para definir as configurações gerais usando o Web Console para um grupo de dispositivos

5. Caso seja necessário especificar um novo formato de nome para os dispositivos do grupo de administração, use o bloco de **Regra de nomeação do grupo de dispositivos** para indicar o novo nome do grupo e as informações adicionais. É possível usar letras maiúsculas e minúsculas dos alfabetos latino e cirílico e caracteres especiais. Um ID exclusivo (oito caracteres) será gerado automaticamente para cada dispositivo no grupo. O número de caracteres no nome do dispositivo não deve exceder 30 caracteres.
6. Mova o botão de alternância localizado à direita no bloco de **Regra de nomeação do grupo de dispositivos** para a posição **Aplicado**.

   Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Aplicado** (Aplicado), os valores definidos dessas configurações serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações não podem ser modificadas na interface do Kaspersky Thin Client. Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Indefinido** (Indefinido), os valores definidos dessas configurações não serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações podem ser modificadas para dispositivos gerenciados na interface do Kaspersky Thin Client em **Dispositivos → Dispositivos gerenciados**.
7. Adicione os detalhes de contato do administrador do Kaspersky Security Center no campo **Detalhes de contato**. É possível especificar o sobrenome, nome, número de telefone e endereço de e-mail do administrador. O número de caracteres nesse campo não deve exceder 80 caracteres.

   Os detalhes de contato do administrador do Kaspersky Security Center são visíveis para o usuário na janela principal do Kaspersky Thin Client, nas janelas para confirmar a redefinição das configurações e dados do Kaspersky Thin Client e confirmar as alterações nas configurações de conexão do Kaspersky Security Center e quando o certificado para conexão com o Kaspersky Security Center for substituído.

8. Mova o botão de alternância localizado à direita no bloco **Suporte Técnico empresarial (administrador)** para a posição **Aplicado**.

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

Configuração de uma conexão com um ambiente remoto do Basis.WorkPlace por meio do Web Console

É possível usar o Web Console para definir as configurações de conexão com um ambiente remoto implementado em uma infraestrutura do Basis.WorkPlace para um dispositivo ou grupo de dispositivos que executam o Kaspersky Thin Client.

As instruções para conectar a um ambiente remoto são fornecidas em um artigo separado.

Como definir as configurações para conexão com um ambiente remoto do Basis.WorkPlace para um dispositivo

1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do thin client onde o Kaspersky Thin Client está em execução. 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 ao grupo **Dispositivos gerenciados**.

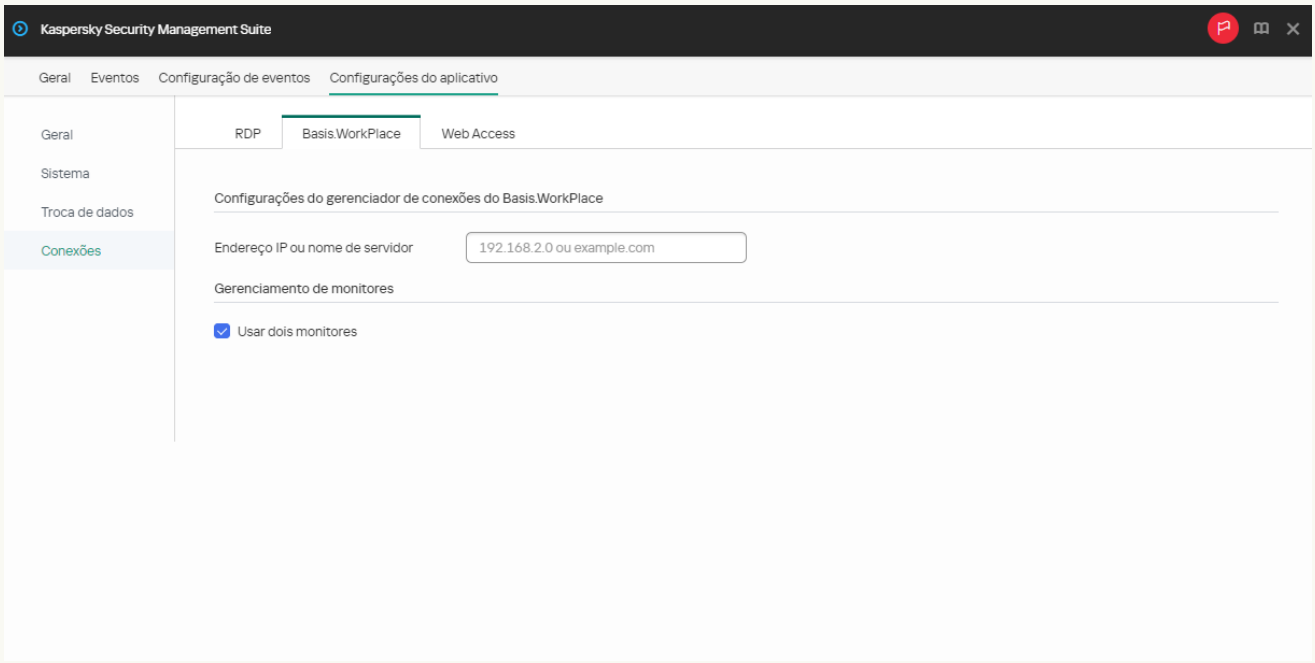
   Caso um dispositivo gerenciado seja adicionado a um grupo de administração e uma política aplicada seja definida para as configurações desse grupo, as configurações definidas individualmente para o dispositivo não serão aplicadas.

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 **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 Basis.WorkPlace (veja a figura abaixo).



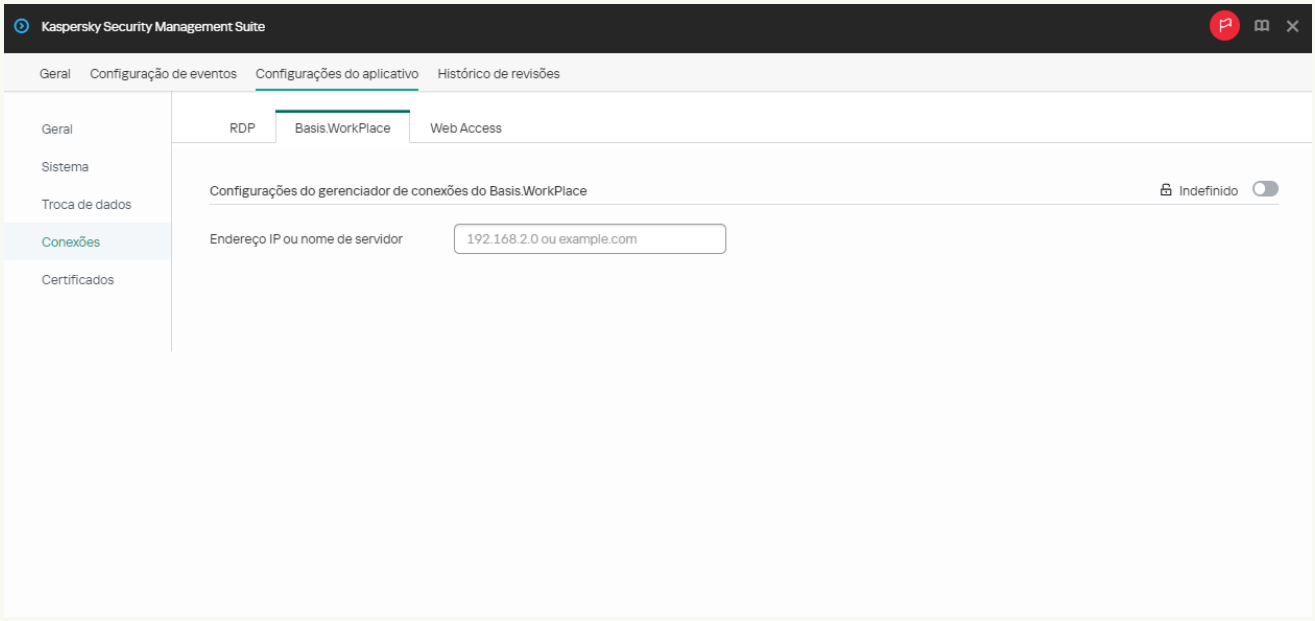
Janela para definir as configurações para conexão com um desktop remoto gerenciado pelo Basis.WorkPlace pelo Web Console para um dispositivo

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 para salvar as alterações.

[Como definir as configurações para conexão com um ambiente remoto do Basis.WorkPlace para um grupo de dispositivos](#)

1. Na janela principal do Web Console, selecione **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**.

   Uma janela será aberta na qual é possível definir as configurações para conexão com um desktop remoto gerenciado pelo Basis.WorkPlace (consulte a figura abaixo).



Janela para definir as configurações para conexão com um desktop remoto gerenciado pelo Basis.WorkPlace pelo Web Console para um grupo de dispositivos

5. Em **Endereço IP ou nome de servidor**, insira o endereço IP ou o nome do servidor ao qual se conectar.
6. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Aplicado** (Aplicado), os valores definidos dessas configurações serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações não podem ser modificadas na interface do Kaspersky Thin Client. Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Indefinido** (Indefinido), os valores definidos dessas configurações não serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações podem ser modificadas para dispositivos gerenciados na interface do Kaspersky Thin Client em **Dispositivos** → **Dispositivos gerenciados**.

Ao trabalhar com o Kaspersky Thin Client por Basis.WorkPlace, as seguintes limitações são aplicáveis:

- Os usuários não podem ser autorizados com cartões inteligentes no gerenciador de conexões Basis.WorkPlace.
- Os usuários não podem iniciar uma alteração de senha no Kaspersky Thin Client.
- A conexão simultânea com vários desktops remotos gerenciados pelo Basis.WorkPlace não é compatível.

Configuração de uma conexão com um ambiente remoto por RDP por meio do Web Console

É possível usar o Web Console para definir as configurações de conexão com um desktop remoto ou um ambiente virtual por RDP para um dispositivo ou um grupo de dispositivos que executam o Kaspersky Thin Client.

As instruções para conectar a um ambiente remoto são fornecidas em um artigo separado.

Como definir as configurações para conexão com o ambiente remoto por RDP para um dispositivo

1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.

2. Clique no nome do thin client onde o Kaspersky Thin Client está em execução. 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 ao grupo **Dispositivos gerenciados**.

   Caso um dispositivo gerenciado seja adicionado a um grupo de administração e uma política aplicada seja definida para as configurações desse grupo, as configurações definidas individualmente para o dispositivo não serão aplicadas.

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

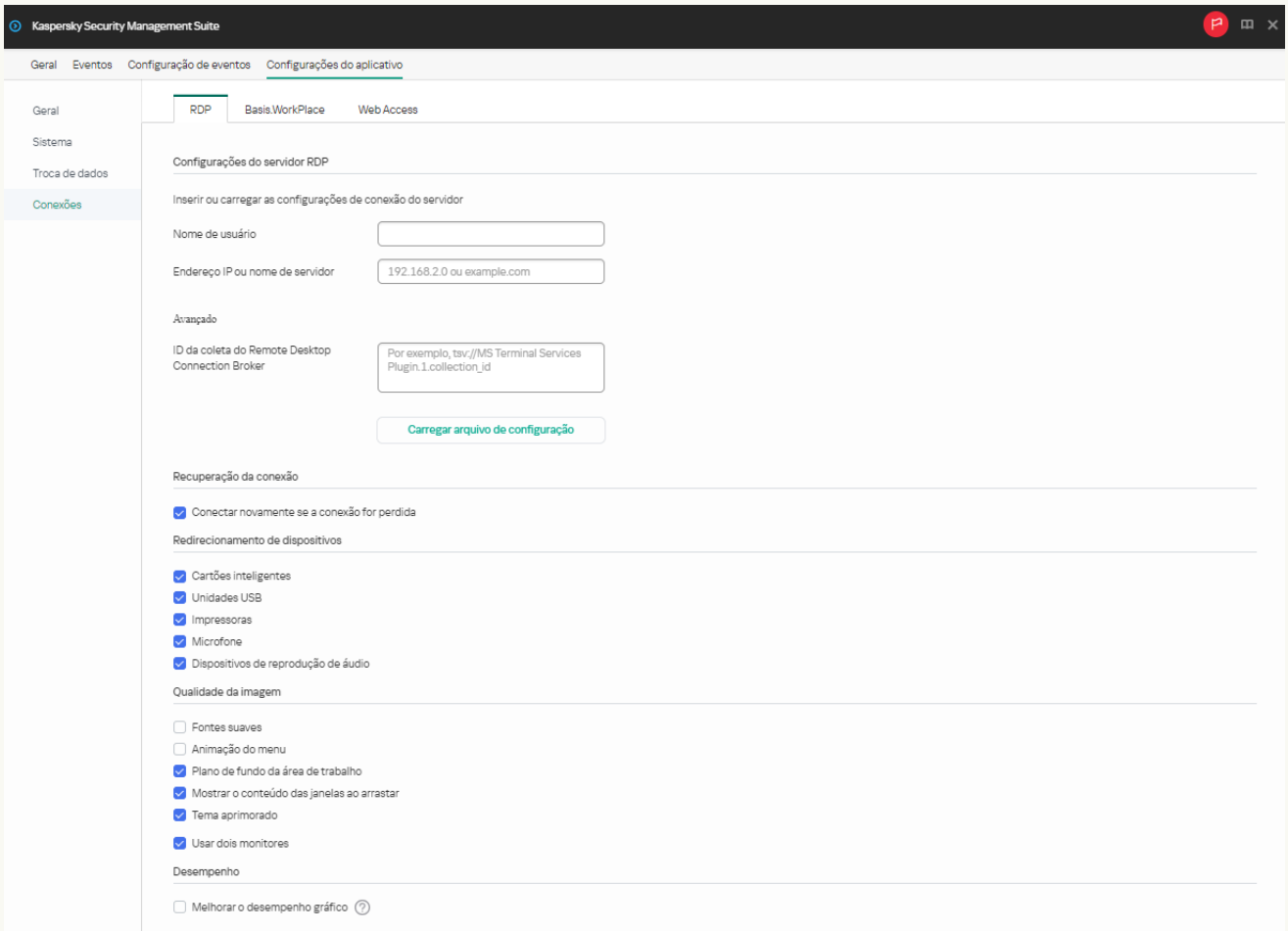
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.

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

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

6. Selecione **Conexões** → **RDP**.

   Uma janela será aberta na qual é possível definir as configurações para conexão com um desktop remoto ou aplicativo virtual por RDP (consulte a figura abaixo).



Janela para definir as configurações para conexão com um desktop remoto por RDP pelo Web Console para um dispositivo

7. No campo **Servidor**, insira o endereço IP ou o nome de 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).

   Especifique um ID da coleta do Remote Desktop Connection Broker para se conectar a um aplicativo virtual.

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

    Especifique um ID da coleta do Remote Desktop Connection Broker para se conectar a um aplicativo virtual.

    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 **Aplicativo**.

11. 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**.

12. No bloco de configurações **Redirecionamento de dispositivos**, ao lado dos dispositivos necessários, marque as seguintes caixas de seleção:

    - **Cartões inteligentes** caso queira ativar o redirecionamento de cartões inteligentes e tokens.
    - **Unidades USB** caso queira ativar o redirecionamento de unidades USB.
    - **Impressoras** caso queira ativar o redirecionamento de impressoras.

      O computador remoto deve ter o driver instalado da impressora conectada ao thin client.
    - **Microfone** caso queira ativar o redirecionamento de dispositivos de registro de áudio.

      O volume do áudio e outras configurações são gerenciados a partir do computador remoto.
    - **Dispositivos de reprodução de áudio** caso queira ativar o redirecionamento de fones de ouvido ou alto-falantes.

      O Kaspersky Thin Client é compatível com a reprodução mono e estéreo. O volume do áudio e outras configurações são gerenciados no ambiente remoto.

13. No bloco **Qualidade da imagem**, marque as caixas de seleção ao lado das configurações gráficas do desktop remoto que precisa usar:

    - **Fontes suaves**
    - **Animação do menu**
    - **Plano de fundo da área de trabalho**
    - **Mostrar o conteúdo das janelas ao arrastar**
    - **Tema aprimorado**

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

14. 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**.

15. Para melhorar o desempenho quando conectado com desktops remotos ou aplicativos, no bloco **Desempenho**, marque **Melhorar o desempenho gráfico**.

    Caso o usuário precise se conectar com um desktop remoto do Microsoft Windows 7, desmarque **Melhorar o desempenho gráfico**. Este recurso não é compatível com conexões com desktops remotos do Microsoft Windows 7.

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

Como definir as configurações para conexão com os ambientes remotos por RDP para um grupo de dispositivos

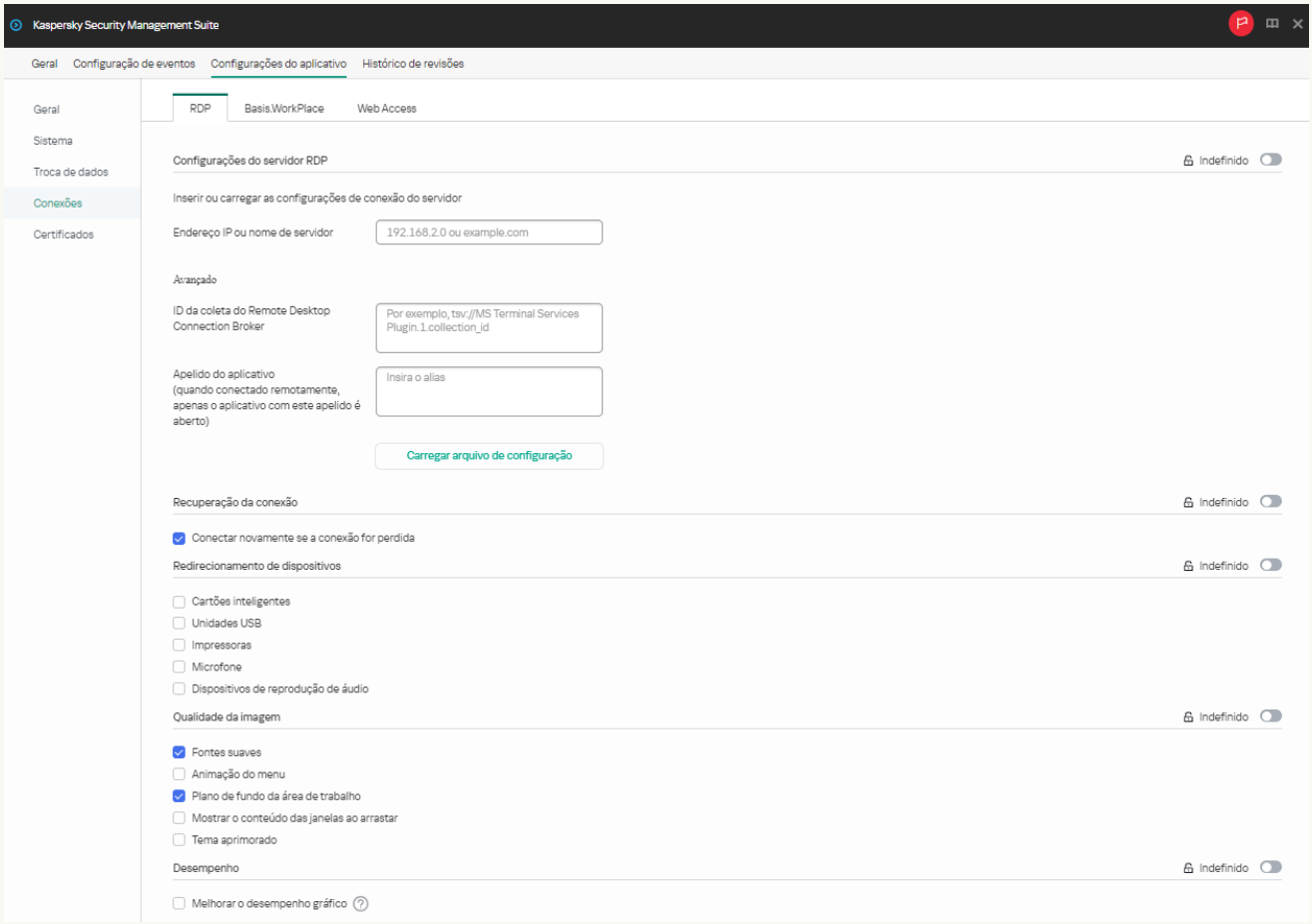
1. Na janela principal do Web Console, selecione **Dispositivos** → **Políticas e perfis**.

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**.

   Uma janela será aberta na qual é possível definir as configurações para conexão com um desktop remoto por RDP (consulte a figura abaixo).



Janela para definir as configurações para conexão com um desktop remoto por RDP pelo Web Console para um grupo de dispositivos

5. No campo **Servidor**, insira o endereço IP ou o nome do servidor para conexão com um desktop remoto por RDP.

6. No campo **Nome de usuário**, insira o nome da conta de usuário que será usada para conexão com um desktop remoto por RDP.

7. 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).

   Especifique um ID da coleta do Remote Desktop Connection Broker para se conectar a um aplicativo virtual.

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

Especifique um ID da coleta do Remote Desktop Connection Broker para se conectar com um aplicativo remoto.

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 **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. No bloco de configurações **Redirecionamento de dispositivos**, ao lado dos dispositivos necessários, marque as seguintes caixas de seleção:

    - **Cartões inteligentes** caso queira ativar o redirecionamento de cartões inteligentes e tokens.
    - **Unidades USB** caso queira ativar o redirecionamento de unidades USB.
    - **Impressoras** caso queira ativar o redirecionamento de impressoras.

      O computador remoto deve ter o driver instalado da impressora conectada ao thin client.
    - **Microfone** caso queira ativar o redirecionamento de dispositivos de registro de áudio.

      O volume do áudio e outras configurações são gerenciados a partir do computador remoto.
    - **Dispositivos de reprodução de áudio** caso queira ativar o redirecionamento de fones de ouvido ou alto-falantes.

      O Kaspersky Thin Client é compatível com a reprodução mono e estéreo. O volume do áudio e outras configurações são gerenciados no ambiente remoto.

11. No bloco **Qualidade da imagem**, marque as caixas de seleção ao lado das configurações gráficas do desktop remoto que precisa usar:

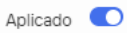
    - **Fontes suaves**
    - **Animação do menu**
    - **Plano de fundo da área de trabalho**
    - **Mostrar o conteúdo das janelas ao arrastar**
    - **Tema aprimorado**

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

12. Para melhorar o desempenho quando conectado com desktops remotos ou aplicativos, no bloco **Desempenho**, marque **Melhorar o desempenho gráfico**.

    Caso o usuário precise se conectar com um desktop remoto do Microsoft Windows 7, desmarque **Melhorar o desempenho gráfico**. Este recurso não é compatível com conexões com desktops remotos do Microsoft Windows 7.

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

Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Aplicado** (), os valores definidos dessas configurações serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações não podem ser modificadas na interface do Kaspersky Thin Client. Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Indefinido** (), os valores definidos dessas configurações não serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações podem ser modificadas para dispositivos gerenciados na interface do Kaspersky Thin Client em **Dispositivos** → **Dispositivos gerenciados**.

Configuração de uma conexão com um ambiente remoto do Web Access por meio do Web Console

É possível usar o Web Console para definir as configurações de conexão com um ambiente remoto no aplicativo Web Access para um dispositivo ou grupo de dispositivos que executam o Kaspersky Thin Client.

No aplicativo Web Access, é possível se conectar a um ambiente remoto implementado nas infraestruturas Citrix Workspace e VMware Horizon por meio da tecnologia HTML5. O navegador Chromium™ é usado para a conexão.

As instruções para conectar a um ambiente remoto são fornecidas em um artigo separado.

Como definir as configurações para conexão com um ambiente remoto no Web Access para um dispositivo

1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do thin client onde o Kaspersky Thin Client está em execução. 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 ao grupo **Dispositivos gerenciados**.

   Caso um dispositivo gerenciado seja adicionado a um grupo de administração e uma política aplicada seja definida para as configurações desse grupo, as configurações definidas individualmente para o dispositivo não serão aplicadas.

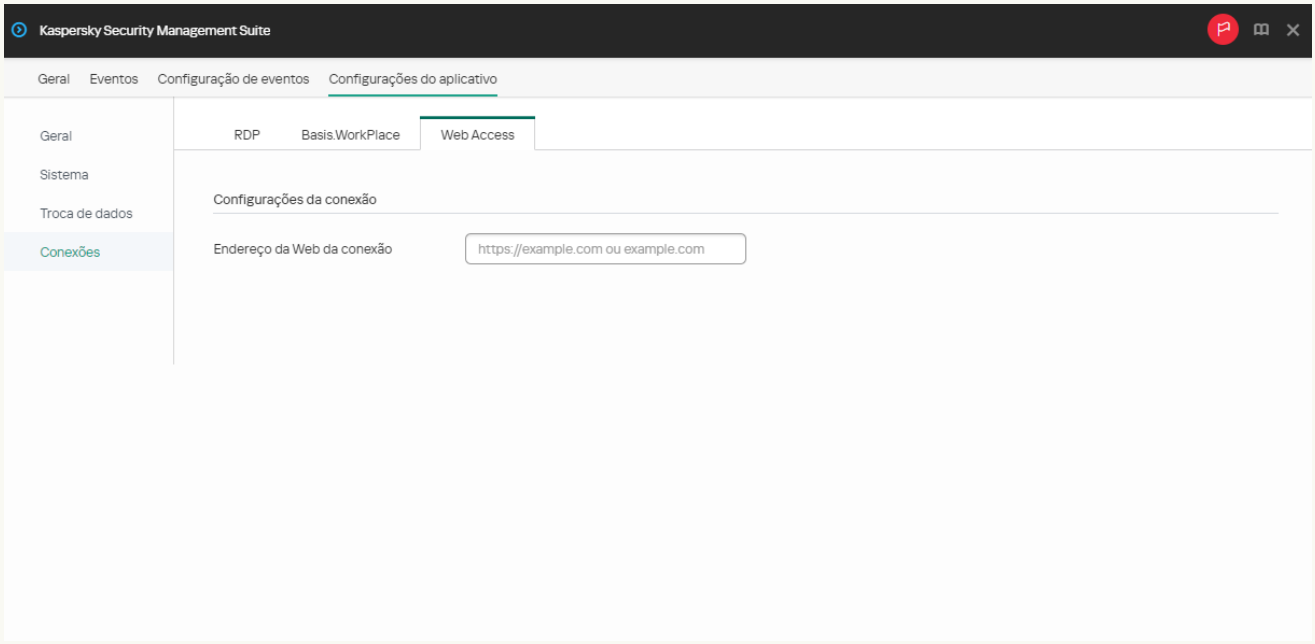
3. Na janela aberta, selecione a guia **Aplicativos**.
4. Clique no nome do plug-in da Web do Kaspersky Security Management Suite.

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

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

   Selecione **Conexões** → **Web Access**.

   A janela para definir as configurações de conexão é aberta (veja a figura abaixo).



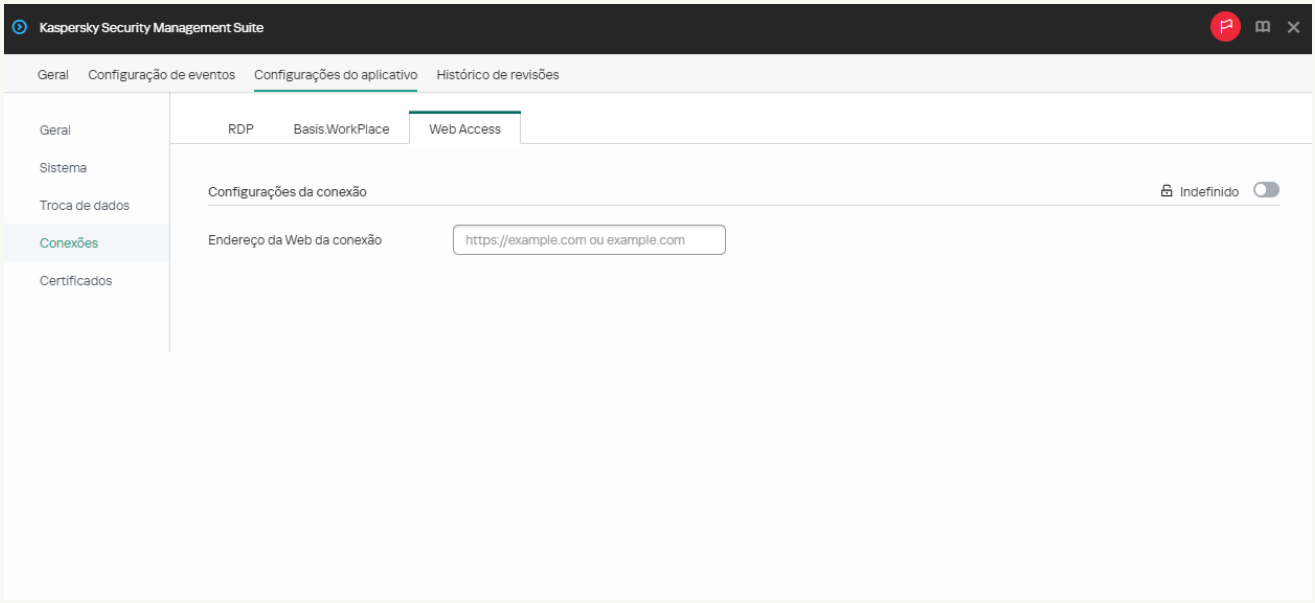
Janela de configuração para conexão com um ambiente no Web Access usando o Web Console

6. No campo **Endereço da Web da conexão**, insira o endereço da Web do servidor para se conectar ao ambiente remoto pertinente.
7. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

Como definir as configurações para conexão com um ambiente remoto no Web Access para um grupo de dispositivos

1. Na janela principal do Web Console, selecione **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**.

   A janela para definir as configurações de conexão é aberta (veja a figura abaixo).



Janela de configuração para conexão com um ambiente remoto no Web Access usando o Web Console

5. No campo **Endereço da Web da conexão**, insira o endereço da Web do servidor para se conectar ao ambiente remoto pertinente.
6. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

O suporte do Kaspersky Thin Client para o desktop remoto do Citrix Workspace tem as seguintes limitações:

- O compartilhamento de arquivos entre o thin client e o desktop remoto não é compatível.
- O compartilhamento da área de transferência entre o thin client e o desktop remoto não é compatível.
- O redirecionamento de unidades USB, cartões inteligentes e tokens USB não é compatível.

Definição das configurações de economia de energia do Kaspersky Thin Client pelo Web Console

No Web Console, é possível definir as configurações de economia de energia para um dispositivo ou um grupo de dispositivos que executam o Kaspersky Thin Client.

Como definir as configurações de economia de energia para um dispositivo

1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.

2. Clique no nome do thin client onde o Kaspersky Thin Client está em execução. 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 ao grupo **Dispositivos gerenciados**.

   Caso um dispositivo gerenciado seja adicionado a um grupo de administração e uma política aplicada seja definida para as configurações desse grupo, as configurações definidas individualmente para o dispositivo não serão aplicadas.

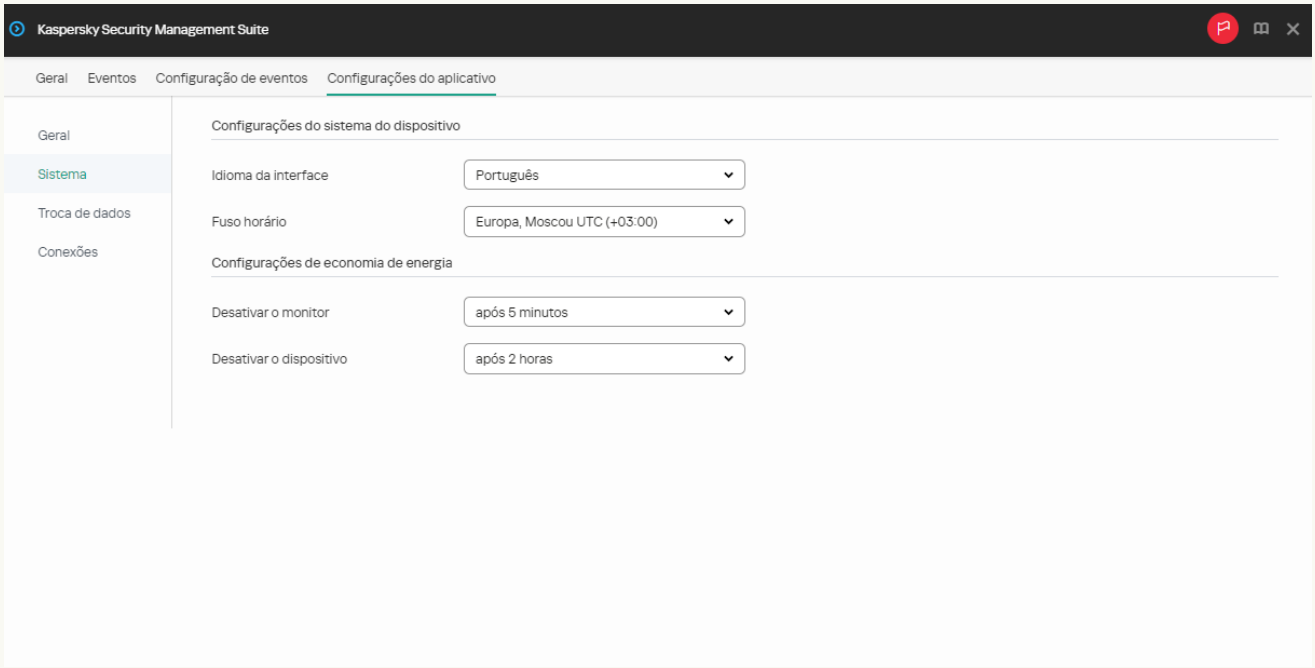
3. Na janela aberta, selecione a guia **Aplicativos**.

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 **Configurações do aplicativo**.

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



Janela para definir as configurações de economia de energia pelo Web Console para um dispositivo

7. No bloco **Configurações de economia de energia**, defina as seguintes configurações:

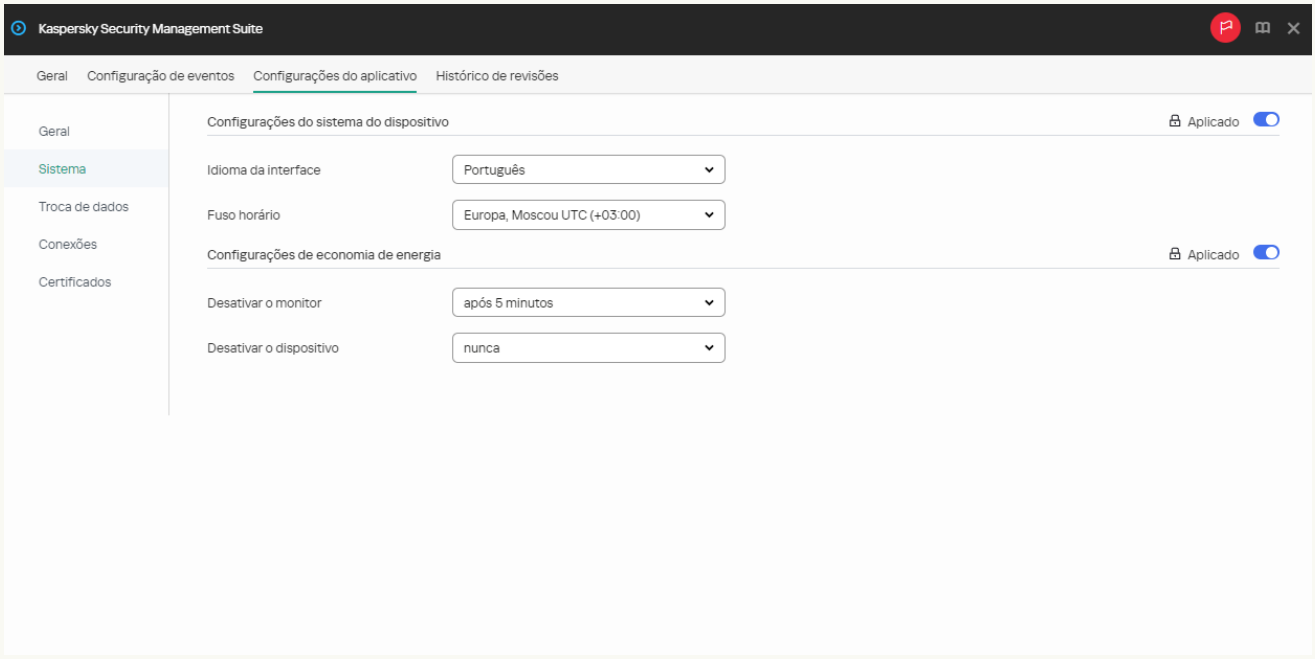
   - Na lista suspensa **Desativar o monitor**, selecione o período de inatividade do sistema após o qual o monitor será desativado.
   - Na lista suspensa **Desativar o dispositivo**, selecione o período de inatividade do sistema após o qual o thin client será desativado.

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

Depois que o Kaspersky Thin Client for sincronizado com o Kaspersky Security Center, as configurações de economia de energia serão aplicadas ao Kaspersky Thin Client.

Como definir as configurações de economia de energia para um grupo de dispositivos

1. Na janela principal do Web Console, selecione **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 de economia de energia pelo Web Console para um grupo de dispositivos

5. 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.
6. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

Depois que todos os dispositivos de um grupo de administração forem sincronizados com o Kaspersky Security Center, as configurações de economia de energia serão aplicadas a todos os Kaspersky Thin Clients incluídos nesse grupo.

Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Aplicado** (Aplicado), os valores definidos dessas configurações serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações não podem ser modificadas na interface do Kaspersky Thin Client. Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Indefinido** (Indefinido), os valores definidos dessas configurações não serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações podem ser modificadas para dispositivos gerenciados na interface do Kaspersky Thin Client em **Dispositivos** → **Dispositivos gerenciados**.

Configuração do idioma da interface e o fuso horário do Kaspersky Thin Client pelo Web Console

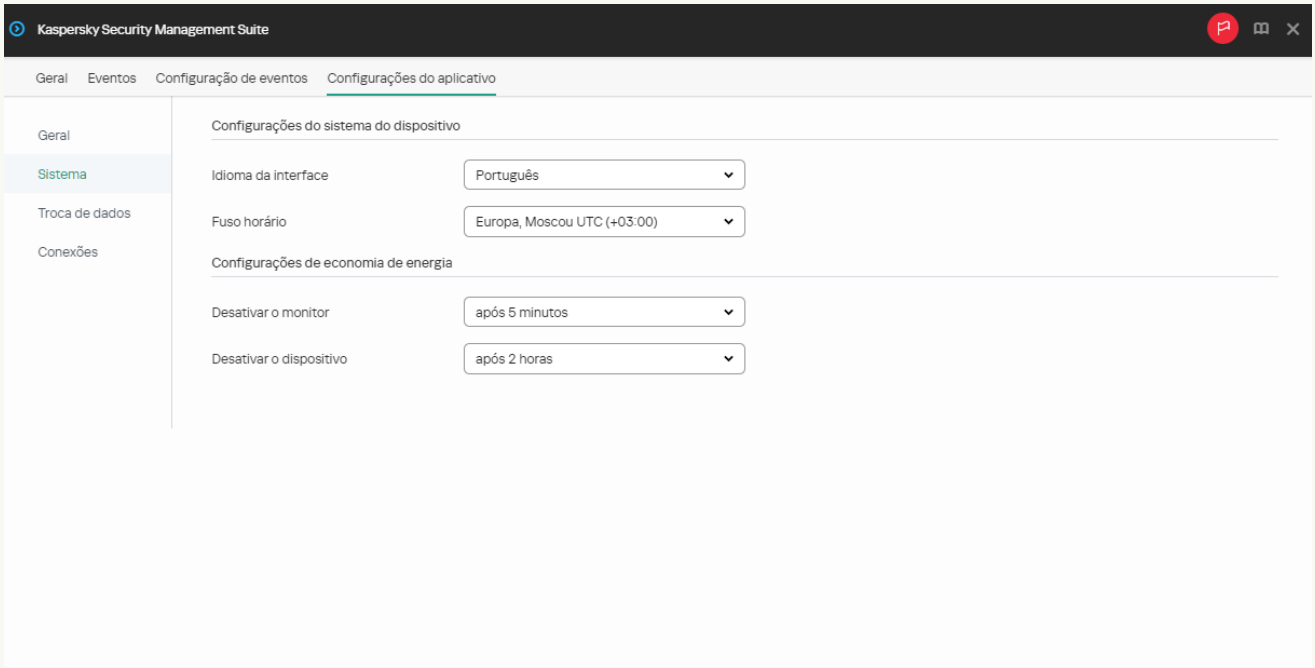
No Web Console, é possível configurar o idioma e o fuso horário da interface para um dispositivo ou um grupo de dispositivos que executam o Kaspersky Thin Client.

Como configurar o idioma e o fuso horário da interface para um dispositivo

1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do thin client onde o Kaspersky Thin Client está em execução. 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 ao grupo **Dispositivos gerenciados**.

   Caso um dispositivo gerenciado seja adicionado a um grupo de administração e uma política aplicada seja definida para as configurações desse grupo, as configurações definidas individualmente para o dispositivo não serão aplicadas.
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 **Configurações do aplicativo**.
6. Selecione a seção **Sistema** (consulte a figura abaixo).

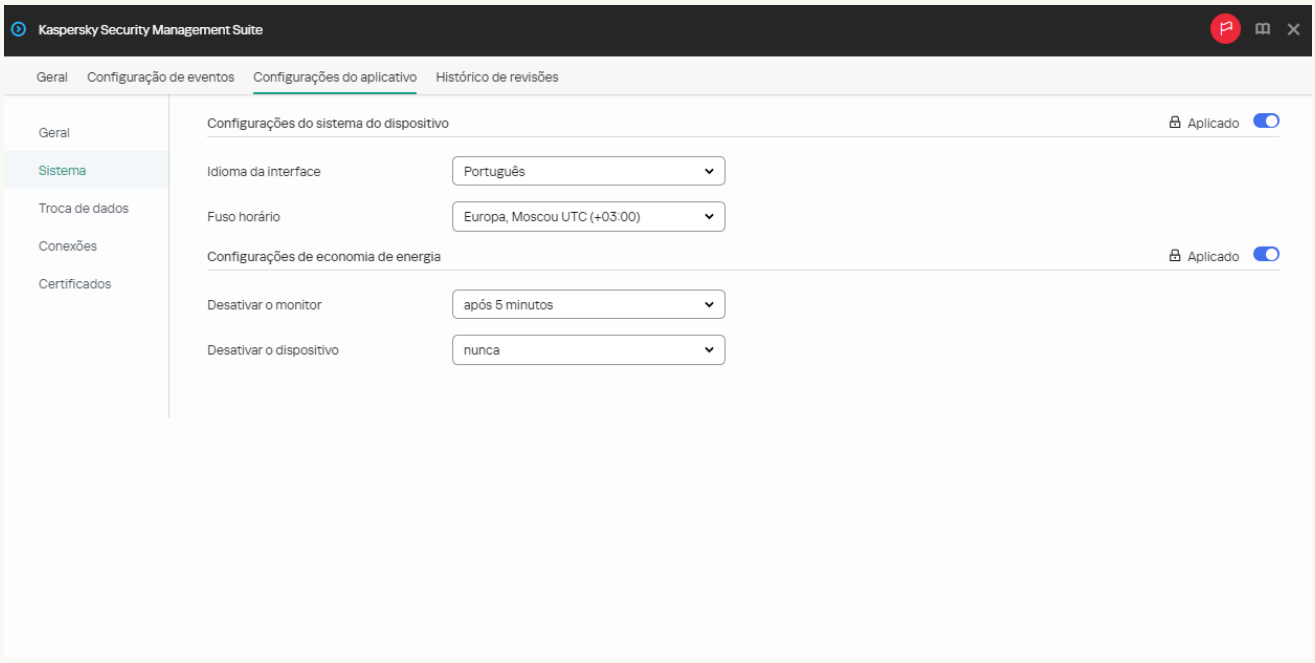


Janela para configurar o idioma e o fuso horário da interface pelo Web Console para um dispositivo

7. No bloco **Configurações do sistema do dispositivo**, selecione os valores relevantes nas listas suspensas **Idioma da interface** e **Fuso horário**.
8. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

Como configurar o idioma e o fuso horário da interface para um grupo de dispositivos

1. Na janela principal do Web Console, selecione **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 configurar o idioma e o fuso horário da interface pelo Web Console para um grupo de dispositivos

5. No bloco **Configurações do sistema do dispositivo**, selecione os valores relevantes nas listas suspensas **Idioma da interface** e **Fuso horário**.
6. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

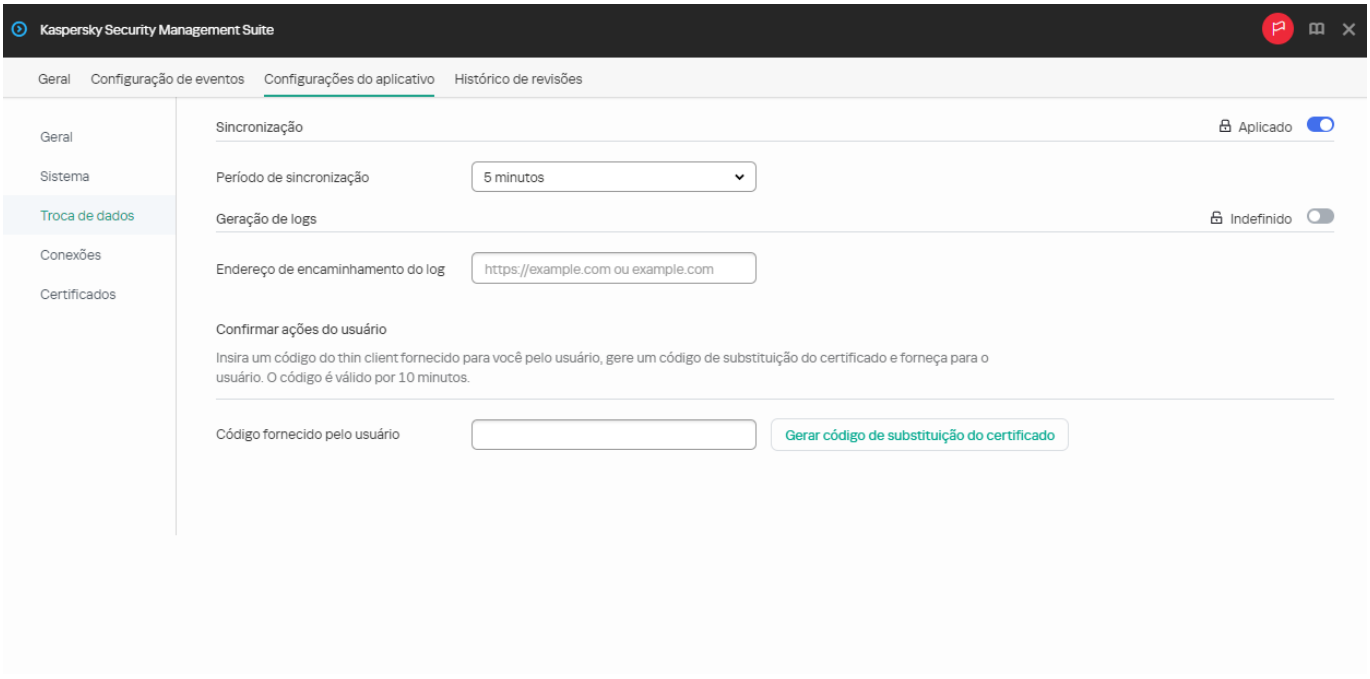
Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Aplicado** (Aplicado), os valores definidos dessas configurações serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações não podem ser modificadas na interface do Kaspersky Thin Client. Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Indefinido** (Indefinido), os valores definidos dessas configurações não serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações podem ser modificadas para dispositivos gerenciados na interface do Kaspersky Thin Client em **Dispositivos** → **Dispositivos gerenciados**.

Configuração da sincronização entre o Kaspersky Thin Client e o Kaspersky Security Center

No Web Console, é possível configurar a sincronização com o Kaspersky Security Center somente para um grupo de dispositivos que executa o Kaspersky Thin Client.

Para configurar a sincronização entre o Kaspersky Thin Client e o Kaspersky Security Center:

1. Na janela principal do Web Console, selecione **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 a sincronização entre o Kaspersky Thin Client e o Kaspersky Security Center

5. No campo **Período de sincronização**, especifique o intervalo para sincronizar o Kaspersky Thin Client com o Kaspersky Security Center.
6. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Aplicado** (Aplicado), os valores definidos dessas configurações serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações não podem ser modificadas na interface do Kaspersky Thin Client. Caso o botão de alternância ao lado do nome de um grupo de configurações esteja na posição **Indefinido** (Indefinido), os valores definidos dessas configurações não serão aplicados aos dispositivos aos quais a política é aplicada, e essas configurações podem ser modificadas para dispositivos gerenciados na interface do Kaspersky Thin Client em **Dispositivos** → **Dispositivos gerenciados**.

Configuração do encaminhamento de logs do Kaspersky Thin Client para um servidor de log

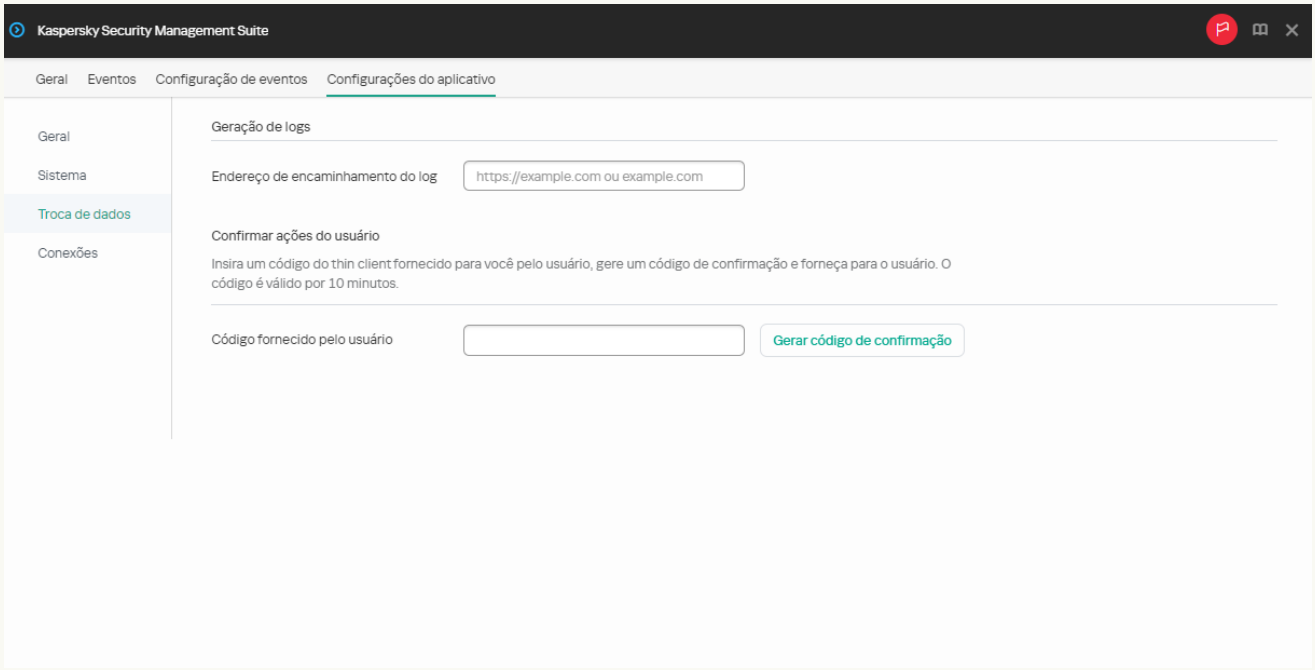
No Web Console, é possível configurar o encaminhamento de logs do Kaspersky Thin Client para um servidor de log para um dispositivo ou um grupo de dispositivos que executam o Kaspersky Thin Client.

Como configurar o encaminhamento de logs para um dispositivo

1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do thin client onde o Kaspersky Thin Client está em execução. 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 ao grupo **Dispositivos gerenciados**.

   Caso um dispositivo gerenciado seja adicionado a um grupo de administração e uma política aplicada seja definida para as configurações desse grupo, as configurações definidas individualmente para o dispositivo não serão aplicadas.
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 **Configurações do aplicativo**.
6. Selecione a seção **Troca de dados** (consulte a figura abaixo).

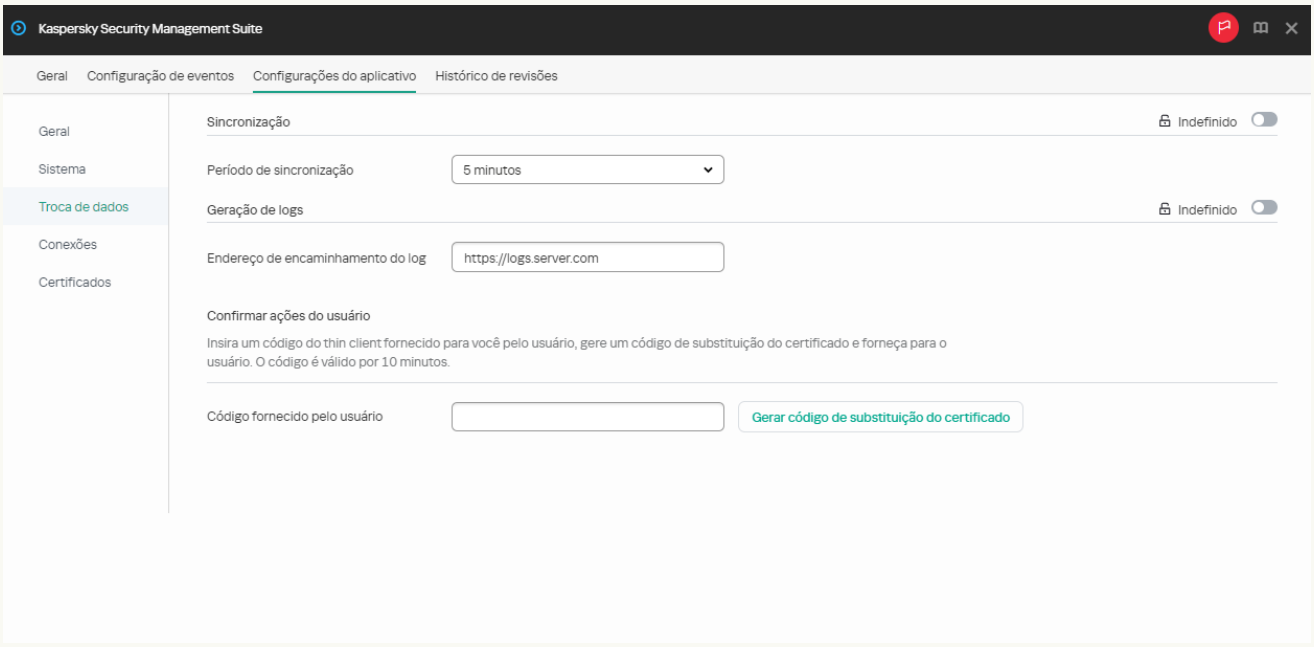


Janela para configurar o encaminhamento de logs do Kaspersky Thin Client pelo Web Console para um dispositivo

7. No campo **Endereço de encaminhamento do log**, insira o endereço do servidor de log de destino no formato https://<endereço do servidor>. Verifique e confirme se um servidor de log em conformidade com os requisitos está implementado na infraestrutura corporativa.
8. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

Como configurar o encaminhamento de logs para um grupo de dispositivos

1. Na janela principal do Web Console, selecione **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 pelo Web Console para um grupo de dispositivos

5. No campo **Endereço de encaminhamento do log**, insira o endereço do servidor de log de destino no formato https://<endereço do servidor>. Verifique e confirme se um servidor de log em conformidade com os requisitos está implementado na infraestrutura corporativa.
6. Clique em **Salvar** na parte inferior da janela para salvar as alterações.

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 com o Kaspersky Security Center ou se estiver conectado, mas não estiver incluído no grupo de dispositivos gerenciados, esse thin client não enviará ao administrador nenhuma solicitação para confirmar as ações listadas acima. Adicione o thin client ao grupo de dispositivos gerenciados para receber solicitações para confirmar as ações do usuário.

Para confirmar a alteração das configurações para conexão com o Kaspersky Security Center ou redefinir todas as configurações do thin client:

1. Na janela principal do Web Console, selecione **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do thin client onde o Kaspersky Thin Client está em execução. 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 ao grupo **Dispositivos gerenciados**.

   Caso um dispositivo gerenciado seja adicionado a um grupo de administração e uma política aplicada seja definida para as configurações desse grupo, as configurações definidas individualmente para o dispositivo não serão aplicadas.

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 **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 **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.

Sugerimos configurar a conexão de um grupo de thin clients a um servidor de log ou a um ambiente remoto usando somente certificados que foram 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 seção *Sobre os certificados* da ajuda on-line do Kaspersky Security Center.

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 ícone ao lado do nome do Servidor de Administração do Kaspersky Security Center.

   A janela de **Propriedades do Servidor de Administração** é aberta.

2. Na lista de subseções, selecione **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 gerenciados e os dispositivos incluídos em um grupo de administração receberão o certificado reemitido para conexão com o Kaspersky Security Center após o Kaspersky Thin Client ser sincronizado 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 usado atualmente 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 ciriar 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 estar familiarizado com os requisitos para certificados do Kaspersky Security Center indicados na seção *Requisitos para certificados personalizados usados no Kaspersky Security Center* da 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 729 -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 729 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. Não há requisitos de senha especiais.

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.

Caso necessário, é possível converter um arquivo de certificado do formato PEM para DER.

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 gerenciados.

É recomendado familiarizar-se com os requisitos para certificados do Kaspersky Security Center da seção *Requisitos para certificados personalizados usados no Kaspersky Security Center* da 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 ícone ao lado do nome do Servidor de Administração do Kaspersky Security Center.

   A janela de **Propriedades do Servidor de Administração** é aberta.

2. Na lista de subseções, selecione **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:

   a. Na lista suspensa **Tipo de certificado**, selecione o **Certificado X.509**.

   b. Caso o certificado do usuário esteja protegido com uma senha, insira a senha.

   c. Selecione o arquivo de certificado do usuário clicando no botão **Procurar** no bloco **Certificado**.

   d. Selecione a chave privada para o certificado do usuário clicando no botão **Procurar** no bloco **Chave privada**.

5. Clique em **Salvar** para salvar o certificado que está sendo adicionado.

6. 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 gerenciados e os dispositivos incluídos no grupo de administração recebem o novo certificado depois que o Kaspersky Thin Client for sincronizado com o Kaspersky Security Center.

Adição de novos certificados no Web Console

Para thin clients membros de um grupo de administração, é possível adicionar certificados ao Web Console para se conectar em um ambiente remoto ou servidor de log.

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 **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, você pode remover certificados de thin clients incluídos 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 **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, salve-o 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 365 -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 a pasta onde 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 de notificações de eventos do Kaspersky Thin Client no 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 seu próprio nível de gravidade. Dependendo das condições de sua ocorrência, um evento pode receber um dos seguintes níveis de gravidade:

- 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 **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 gravidade dos eventos cujas informações o usuário deseja receber:
   - **Crítico**
   - **Falha funcional**
   - **Advertência**
   - **Informações**

   Uma tabela de eventos para o nível de gravidade selecionado será exibida.
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 gravidade especificada para o Servidor de Administração do Kaspersky Security Center. O tempo de armazenamento padrão dos eventos é de 30 dias.

Como configurar as notificações de eventos para um grupo de dispositivos

1. Na janela principal do Web Console, selecione **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 gravidade dos eventos cujas informações o usuário deseja receber:
   - **Crítico**
   - **Falha funcional**
   - **Advertência**
   - **Informações**

   Uma tabela de eventos para o nível de gravidade selecionado será exibida.
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 gravidade 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 quanto a configuração das notificações para registro de eventos no Kaspersky Security Center Web Console, consulte a seção *Configurar a entrega de notificações* do guia de 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 **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** exibe a data e a hora nas quais o Web Console recebeu o evento registrado em um dispositivo.
- **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.
- **Nível de gravidade** exibe a gravidade do evento (*Crítico*, *Falha funcional*, *Advertência* ou *Informações*).
- **Tarefa** exibe um nome da tarefa a ser executada quando o evento é registrado.
- **Registrado** exibe a data e a hora nas quais o evento foi registrado no dispositivo.

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 desktop 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 e/ou o log de eventos.

Desconexão do desktop remoto

Se você encontrar um erro que faça com que o Kaspersky Thin Client se desconecte de um desktop remoto, uma conexão será restabelecida automaticamente se esta opção estiver ativada nas configurações de conexão do ambiente remoto.

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 operação no desktop remoto:

1. Feche a mensagem de erro.
2. Tente estabelecer conexão com o desktop remoto.
3. Caso a conexão falhe, reinicie o thin client e tente se conectar com o desktop remoto novamente.
4. Caso ainda não seja possível estabelecer uma conexão, entre em contato com o administrador de sua empresa para corrigir quaisquer problemas físicos que possam estar fazendo com que o Kaspersky Thin Client se desconecte do desktop remoto.
5. 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.

Teste da conexão de rede

Para testar se o thin client está conectado à rede,

Visualize o status da conexão de rede do Kaspersky Thin Client no painel de controle do Kaspersky Thin Client.

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 dados sobre os certificados carregados no Kaspersky Thin Client e contém informações sobre as instâncias em que o Kaspersky Security Center foi usado para ativar ou desativar o gerenciamento de thin clients. 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.

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.

O log de auditoria do Kaspersky Thin Client contém as seguintes informações:

- Data e hora de upload do certificado para conectar o Kaspersky Thin Client ao Kaspersky Security Center.
- Endereço do Servidor de Administração do Kaspersky Security Center (endereço IP e/ou nome do servidor de domínio).
- Número da porta do Servidor de Administração do Kaspersky Security Center.
- 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, ID do thin client.
- Informações sobre incidentes quando o gerenciamento do Kaspersky Thin Client pelo Kaspersky Security Center Web Console foi ativado ou desativado.

Encaminhamento do log

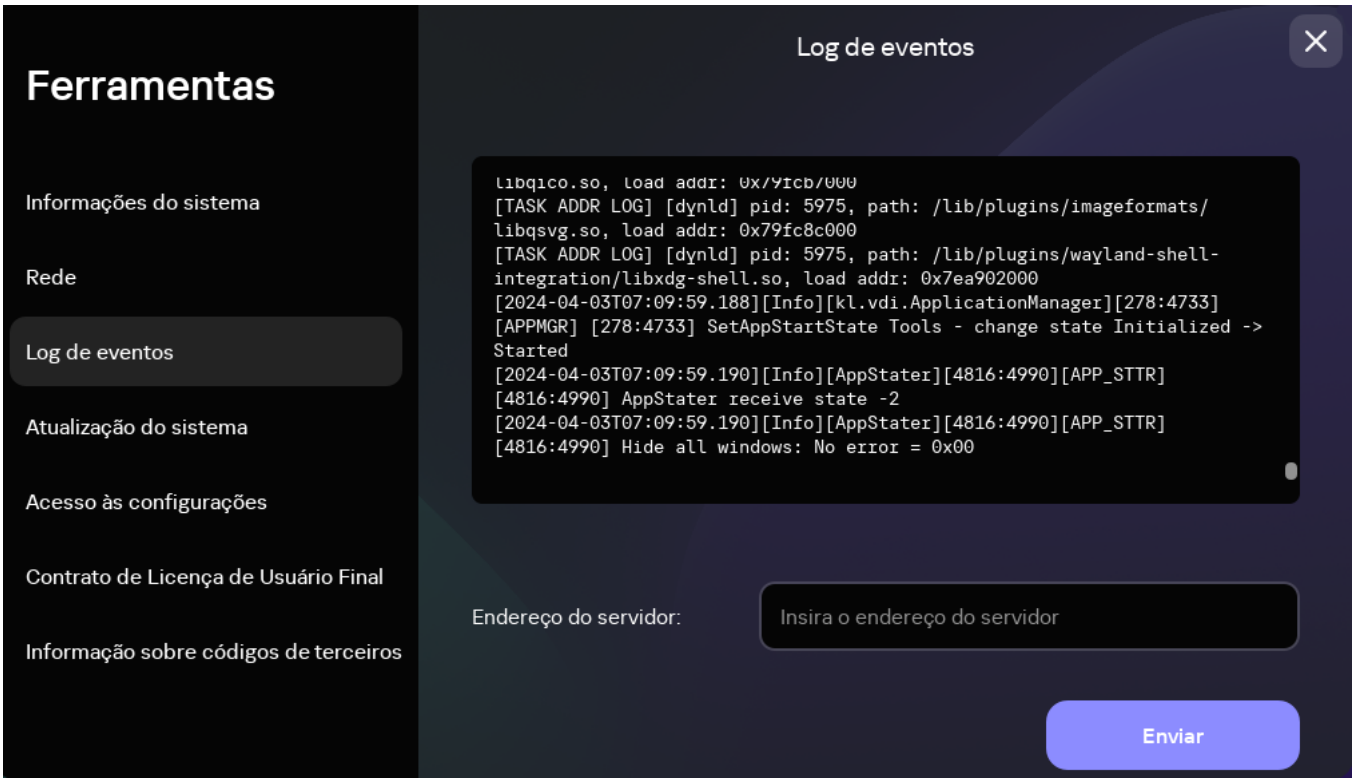
Ao entrar em contato com o Suporte Técnico, os especialistas da Kaspersky podem solicitar que você forneça logs de eventos e de auditoria. Na interface do Kaspersky Thin Client, você pode encaminhar logs para um servidor de log, de onde os especialistas possam baixá-los.

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 **Log de eventos** (consulte a figura abaixo).



Ferramentas. Seção Log de eventos

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 Kaspersky Thin Client seja membro de um grupo de administração, seja controlado centralmente pelo Web Console e a função **Aplicado** esteja ativada, o campo **Endereço do servidor** conterá o valor definido pelo administrador do Kaspersky Security Center que não pode ser alterado.

   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 podem ser enviados para terceiros não autorizados. Se esse for o caso, a confidencialidade dos dados que eles contêm podem ficar comprometidas.

4. Na janela aberta, confirme se deseja encaminhar os logs de auditoria e de eventos.

   Caso o Kaspersky Thin Client não esteja em um grupo de administração e caso os logs de auditoria e de eventos estejam sendo encaminhados para um servidor de log pela primeira vez, verifique as configurações do certificado que está sendo adicionado na janela aberta **Adicionar 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.

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.

Aplicativo virtual

Aplicativo implementado em um servidor remoto e que requer o uso de tecnologias de acesso remoto para se conectar com ele.

Atualização

Um procedimento para substituir/adicionar novos arquivos (bancos de dados ou módulos do Kaspersky Thin Client) recebidos dos servidores de atualização da Kaspersky.

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.

Dispositivos gerenciados

Dispositivos de rede corporativa incluídos em um grupo de administração.

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 combinados de acordo com as funções executadas. Os dispositivos são agrupados para facilitar o gerenciamento como um todo. Um grupo pode incluir outros grupos. As políticas de grupo podem ser criadas para cada thin client adicionado a um grupo.

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 configuração do 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.

Servidores de atualização da Kaspersky

Servidores HTTP da Kaspersky a partir dos quais um aplicativo da Kaspersky recebe atualizações de bancos de dados e módulos do aplicativo.

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.

Web Access

Aplicativo para conexão com um ambiente remoto usando a tecnologia HTML5. A versão atual do Kaspersky Thin Client no Web Access é compatível com a conexão com desktops virtuais implementadas usando a infraestrutura Citrix Workplace e VMware Horizon.

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 Workplace são marcas comerciais da Citrix Systems, Inc. e/ou uma ou mais de suas subsidiárias e podem estar registradas no Escritório de Marcas e Patentes dos Estados Unidos e em outros países.

Chromium é uma marca comercial da Google LLC.

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.

VMware Horizon é uma marca registrada ou marca comercial da VMware, Inc. nos Estados Unidos e/ou em outras jurisdições.